Die Fundamental-Classen der zusammensetzbaren arithmetischen Formen.

Von

Ernst Schering.

Der Königl. Gesellschaft der Wissenschaften überreicht am 11. Juli 1868.

Der Begriff der Zusammensetzung oder Composition arithmetischer Formen ist von Gauss eingeführt und zwar zunächst für die binären quadratischen Formen. Die Untersuchungen, die er diesem Gegenstande gewidmet hat, bilden einen sehr umfangreichen Theil seiner ,,Disquisitiones Arithmeticae" 1801, und gehören zu den schönsten und fruchtbarsten Gebieten, welche der Wissenschaft durch dieses Werk eröffnet sind. Der Hauptlehrsatz, der die Uebertragung des Begriffs der Composition von den Formen auf die Classen der letztern gestattet, dass nemlich die Classe einer Form, welche aus andern Formen durch Zusammensetzung entstanden ist, allein von den Classen abhängt, denen die einzelnen bei der Zusammensetzung angewandten Formen angehören, wird von Gauss durch eine einzige Entwickelung unmittelbar in der vollständigsten Allgemeinheit bewiesen. Eine bedeutende Vereinfachung im Gedankengange und in den anlytischen Entwickelungen entsteht, wenn man von dem Falle ausgeht, in welchem die zusammenzusetzenden Formen eigentlich primitiv sind, gleiche mittlere Coëfficienten und als erste Coëfficienten relative Primzahlen enthalten. Dirichlet hat diese Untersuchung in einer eignen Abhandlung ,,De formarum binariarum secundi gradus compositione", 1851, durchgeführt; aber auch der hier gegebene Beweis lässt sich noch vereinfachen, wie auch Herr Kronecker bemerkt hat, wenn man von vier eigentlich primitiven paarweise einander aequivalenten Formen, deren mittlere Coëfficienten einander gleich, deren erste Coëfficienten zu einander relativ prim sind, ausgeht und wenn man die Composition zweier dieser Formen, über deren Aequivalenz oder Nichtaequivalenz keine Voraussetzung gemacht ist, vergleicht mit der Composition der beiden andern diesen einzeln aequivalenten Formen.

In den Disquiss. Arr. gibt Gauss die Eintheilung der Classen in Genera leitet mit Hülfe der Lehre von der Composition der Formen eine obere Grenze für die Anzahl dieser Geschlechter ab und erhält dadurch das Hülfsmittel zu einem Beweise des Reciprocitäts-Satzes für die quadratischen Reste. Die vollständige Bestimmung der Anzahl der Geschlechter leitet Gauss in jenem Werke aus der Lehre von der Composition der Formen und der Theorie der ternären quadratischen Formen ab. Dieselbe Bestimmung gibt Dirichlet 1839 in seinen „Recherches sur diverses applications de l'analyse infinitésimale à la théorie des nombres“ auf einem ganz verschiedenen Wege ohne jene beiden Gebiete der Zahlentheorie zu berühren.

Die Lehre von der Composition der Classen bietet Gauss ein Mittel dar zu noch einer andern Eintheilung und Anordnung derselben nemlich nach Perioden, von denen jede alle die Classen umfasst, welche durch wiederholte Composition aus irgend einer in derselben entstehen können. Diejenigen Determinanten deren sämmtliche Classen des sogenannten Haupt-Geschlechts in einer einzigen Periode dargestellt werden, nennt Gauss reguläre, die andern irreguläre, und für diese bestimmt er Exponenten der Irregularität. Einige Eigenschaften dieser Exponenten werden in den Disquiss. Arr. art. 306. VIII ohne Beweis aufgestellt sowie auch einige Andeutungen über eine zweckmässige Auswahl der Perioden in art. 306. IX gegeben. Unter Gauss handschriftlichem Nachlasse findet sich für die Durchführung dieser Untersuchung ein kurzer wahrscheinlich im Jahre 1801 aufgezeichneter Anfang „Démonstration de quelques théorèmes concernants les périodes des classes des formes binaires“, den ich im II. Bande von Gauss Werken habe abdrucken lassen. Meine hier vorliegenden Untersuchungen, die auch jene Fragen mit erledigen, folgen einen anderen als den in jenem Anfang zu einer Abhandlung erkennbaren Weg. Aus mehren Gründen habe ich aber geglaubt, meine im Jahre 1855 von der Gaussischen Arbeit unabhängig gefundene Methode in der folgenden Darstellung beibehalten zu müssen.

Der hier bewiesene Lehrsatz, dass es für jede Determinante solche Classen gibt, die ich Fundamental-Classen genannt habe, durch deren wiederholte Zusammensetzung mit einander jede Classe der Determinante entsteht und zwar jede nur auf Eine Weise, wenn man von einer Classe nicht mehr Compositionen zulässt als ihre Periode Classen enthält, bietet vielfache Anwendung. Mit Hülfe dieses Satzes und der Beziehung zwischen der Anzahl der Fundamental-Classen, denen gerade Perioden-Zahlen zugehören, und der Anzahl der Geschlechter der Formen habe ich nach Vorbild des von Dirichlet in den Monatsberichten der Berliner Academie der Wissenschaften für den speciellen Fall regulärer Primzahl-Determinanten gegebenen Beweises, allgemein nachgewiesen, dass jede eigentlich primitive Form unendlich viele Primzahlen darstellt. Ein Satz welcher mir in meiner Abhandlung ,,Théorèmes relatifs aux formes binaires quadratiques qui représentent les mêmes nombres" Liouville, Journal t. 24. 1859, dazu gedient hat, zuerst strenge zu beweisen, dass zwei primitive Formen, welche dieselben Zahlen darstellen, einander eigentlich oder uneigentlich äquivalent sein müssen.

Mit Hülfe der Eigenschaften der Fundamental-Classen lässt sich auch der von Dirichlet in einer Notiz der Comptes rendus hebdomadaires 1840 Febr. 17 angedeutete Satz beweisen dass eine eigentlich primitive binäre quadratische Form auch unendlich viele solche Primzahlen darstellt, die zugleich in einer beliebig bestimmten, mit den Characteren des Geschlechts jener quadratischen Form verträglichen, linearen Form enthalten sind.

Die Fundamental-Classen bieten die Möglichkeit, eine Tabelle der zu gegebenen Determinanten zugehörigen Classen aufzustellen, ohne dafür einen zu grossen Raum in Anspruch zu nehmen und doch die zum Gebrauch der Tabelle noch erforderliche Hülfsrechnung auf ein geringes Maass zu beschränken, wenn man z. B., wie ich es bei den Berichtigungen der Gauss'schen Tafeln der Anzahl der Classen gegebener Determinanten G. W. B. II. S. 498 ausgeführt habe, neben jeder Determinante die Periodenzahlen der Fundamental-Classen und die durch diese dargestellten kleinsten Primzahlen verzeichnet.

Die Theorie der arithmetischen Formen ist durch Herrn Kummers Entdeckung der idealen Zahlen auch schon auf solche Formen beliebigen Grades ausgedehnt, welche sich mit Zuhülfenahme allein der aus Wurzeln der Einheit entstehenden Irrationalitäten in lineare Factoren zerlegen lassen, und von Herrn Kronecker haben wir die Veröffentlichung einer Theorie der allgemeinen zerlegbaren Formen jedes Grades zu hoffen. Für diese Formen gelten, wie Herr Kummer in seiner Abhandlung aus dem Jahre 1859 „Ueber die allgemeinen Reciprocitätsgesetze unter den Resten und Nichtresten der Potenzen, deren Grad eine Primzahl ist" hervorhebt, analoge Sätze wie für die binären quatrischen Formen in Bezug auf die Composition und zwar, wie sich aus dieser Untersuchung ergibt, diejenigen Sätze welche die Aufstellung von Fundamental-Classen ermöglichen.

Die Definition der idealen Zahlen kann in der Weise festgesetzt werden, dass in Bezug auf die hier zunächst in Betracht kommenden Eigenschaften diejenigen Formen, welche den eigentlich idealen Zahlen im Gegensatze zu den wirklichen aus denselben Irrationalitäten gebildeten Zahlen zugehören, den binären quadratischen Formen einer von der Haupt-Classe verschiedenen Classe entsprechen und die den wirklichen Zahlen angehörenden Formen den binären quadratischen Formen der Haupt-Classe entsprechen. Um eine gemeinsame Bezeichnung zu haben, will ich dem gemäss hier die Benennungen von Haupt-Classen und Nicht-Haupt-Classen der allgemeinen Formen gebrauchen.

1.

Die wesentlichste Eigenschaft der in lineare Factoren zerlegbaren Formen in Bezug auf ihre Composition drückt der von Herrn Kummer in §. 6 seiner Abhandlung „Ueber die allgemeinen Reciprocitäts-Gesetze u. s. w." angegebene Satz aus, der sich nach den eben aufgestellten Bestimmungen so aussprechen lässt, dass die Classe der durch Zusammensetzung zweier Formen entstandenen Form allein von den Classen jener beiden Formen abhängt, dass demnach der Begriff der Composition von den Formen auf ihre Classen übertragen werden kann. Aus der Endlichkeit der Anzahl der Classen derjenigen Formen, deren lineare Factoren zusammengehörige Irrationalitäten enthalten, folgt dann der am selben Orte aufgestellte Satz, dass jede Classe durch wiederholte Zusammensetzung mit sich selbst eine Reihe von Classen hervorbringt, die in gleiche Perioden getheilt werden kann, welche als erstes Glied jene Classe als letztes Glied die Haupt-Classe und überhaupt nur solche Classen enthält, welche alle von einander verschieden sind.

Gibt es eine Periode, welche alle überhaupt zusammengehörigen Classen, also, wenn es binäre quadratische Formen sind, alle Classen derselben Determinante, die Gauss dann eine reguläre Determinante nennt, umfasst, so ist die Anfangs-Classe der Periode eine selbständige Fundamental-Classe. Diese Periode hat dann eine so grosse Anzahl von Gliedern, dass die Anzahl von keiner anderen Periode übertroffen wird.

Erschöpft die grösste Periode aber noch nicht alle mit einander zusammensetzbaren Classen, so kommt es darauf an, zu untersuchen, ob Perioden vorhanden sind, die unter sich und mit jener ersteren keine andere Classe als die Haupt-Classe gemeinsam haben, aus denen auch durch Zusammensetzung von je einer Classe aus jeder Periode keine Classe auf zwei verschiedene Weisen, das heisst abgesehen von einer Vertauschung der Reihenfolge der Zusammensetzung, abgeleitet werden kann.

2.

Sucht man neben der einen grössten Periode oder neben einer unter den etwa vorhandenen mehreren gleichzahligen grössten beliebig ausgewählten Periode eine solche Periode auf, die mit jener ersten ausser der Haupt-Classe keine andere Classe gemeinsam hat, und die durch Zusammensetzung einer ihrer Classen mit einer der ersten Periode keine Classe auf zwei oder mehre verschiedene Weise hervorbringt und die endlich unter allen Perioden, welche solche Bedingungen erfüllen, die grösste Anzahl von Classen enthält, so erkennt man daraus den Weg, den man dann, wenn diese beiden Perioden mit ihren Zusammensetzungen noch nicht alle Classen umfassen, einschlagen muss, um eine dritte Periode von analoger Eigenschaft zu finden.

Wir wollen daher, um allgemein die Regel für die Fortsetzung einer solchen Reihe von Perioden zu finden, annehmen, es seien *solche Classen* A, B, C, . . . F, . . I, L, M *gegeben, deren jede z. B.* F *selbst sowie jede Classe in ihrer Periode mit Ausnahme der Haupt-Classe von den durch Zusammensetzung aus den vorangehenden Classen entstehenden Classen verschieden ist, und die zugleich unter den Classen mit dieser selben Eigenschaft die grösste oder eine der etwa gleichen grössten Periodenzahl besitzt.* Zunächst folgt, dass durch diese Bedingung auch diejenige erfüllt ist, dass *keine Classe auf zwei verschiedene Arten durch Zusammensetzung aus* A, B, C . . F, . . L, M, *entstehen kann.* Bei dem Beweise stellt es sich als vortheilhaft heraus, dem von Gauss für die Composition angewandten $+$ Zeichen entsprechend auch das $-$ Zeichen einzuführen. Aus der Art wie die Periode einer Classe $(+C)$ gebildet wird, folgt, dass es eine Classe, die mit $-C$ zu bezeichnen ist, gibt, mit welcher die erstere $+C$ zusammengesetzt die Haupt-Classe K entstehen lässt. Da nun durch Zusammensetzung einer Classe mit einer Haupt-Classe jene erstere ungeändert bleibt, so gelten für den Gebrauch jener Zeichen auch die für die algebraischen Operationen bekannten Regeln. Würde eine Classe auf verschiedene Weise durch Zusammensetzung aus A, B, . . . L, M z. B. durch

$$\alpha A + \beta B + \ldots + \lambda L + \mu M \text{ und } \alpha' A + \beta' B + \ldots + \lambda' L + \mu' M$$

entstehen, so müsste:

$$(\alpha - \alpha') A + (\beta - \beta') B + \ldots + (\lambda - \lambda') L = (\mu' - \mu) M$$

sein, also nach der Voraussetzung $\alpha - \alpha'$, $\beta - \beta'$, . . . $\lambda - \lambda'$, $\mu' - \mu$ beziehungsweise durch die Periodenzahlen der Classen A, B, . . L, M, theilbar sein, was der Voraussetzung widerspricht, dass jene beiden Darstellungen einer und derselben Classe von einander verschiedene seien.

3.

Die Classe A besitzt die grösste Periodenzahl, die überhaupt bei einer der hier zu betrachtenden Classen vorkommt, würde sie durch ihre wiederholte Composition mit sich selbst alle diese Classen ergeben, so folgte unmittelbar, dass sie durch die Periodenzahl jeder anderen Classe theilbar sein würde. Dieser Satz gilt auch in dem vorliegenden Falle, wie Herr Kummer bemerkt hat, und ergibt sich nach der von Gauss in art. 306. VII der Disquiss. Arr. angewandten Methode, um aus zwei Perioden eine dritte abzuleiten.

Für die Classen C und G seien c und g die Periodenzahlen, h die kleinste durch c und g theilbare Zahl, c' und g' die grössten Zahlen, die unter sich relativ prim sind und beziehungsweise die Zahlen c und g theilen, so dass also nach art. 73 der Disquiss. Arr. $c'g' = h$ wird. Bildet man die Classe $H = \frac{c}{c'}C + \frac{g}{g'}G$, so besitzt die Classe H eine Periodenzahl, welche h theilen und durch c' und g' theilbar sein muss, das ist h selbst. Aus diesem Verfahren ergibt sich unmittelbar, dass die grösste Periodenzahl, die bei zusammengehörigen Classen vorkommt, theilbar ist durch die Periodenzahl jeder der anderen Classen.

Bezeichnet a die Periodenzahl der Classe A und g jetzt die Periodenzahl irgend einer Classe G, so ist also a durch g theilbar. Wird aber schon für ein g', welches die kleinste derartige Zahl sein mag, die Classe $g'G$ durch eine wiederholte Composition $a'A$ der Classe A mit sich selbst dargestellt, so muss der grösste gemeinsame Theiler δ von g' und a auch ein Theiler von a' sein, weil $\frac{g'}{\delta} a G = K$ und $g' \frac{a}{\delta} G = a' \frac{a}{\delta} A$ ist. Man kann also zwei Zahlen γ und α bestimmen, so dass $\gamma g' = a' + \alpha a$ wird, dann hat die Classe $\gamma A - G = G'$, wie leicht zu sehen, die Periodenzahl g' und diese muss nach dem eben Bewiesenen ein Theiler von a und demnach auch von a' sein, d. h. *diejenige kleinste Zahl g', welche solche Composition irgend einer Classe G angibt, die auch durch eine wiederholte Composition $a'A$ der Classe A von der grössten Periodenzahl a entsteht, theilt die Zahl a'.*

Der entsprechende Satz für unsere Reihe von Classen $A, B, C \dots . I, L, M$ würde darin bestehen, dass die kleinste Zahl, welche von irgend einer Classe diejenige wiederholte Composition bezeichnet, die in jene Classen zerlegt werden kann, sowol die Periodenzahlen von $A, B, C \dots . I, L, M$ als auch die Zahlen theilt, welche die von jeder dieser Classen dabei angewandten wiederholten Compositionen bestimmen.

Wir wollen voraussetzen, dass dieser Satz für die Classen $A, B, C \dots I, L$ erfüllt ist und zeigen, dass er auch für M noch mit eingeschlossen gilt.

4

Es sei R eine Classe, die nicht in $A, B, C \dots F \dots I, L, M$ zerlegt werden kann, r' die kleinste Zahl, die angibt, die wie vielste Zusammensetzung von R mit sich selbst in Classen jener Reihe zerlegt werden kann und zwar sei

$$r'R = \alpha' A + \beta' B + \dots + i' I + \lambda' L + \mu' M$$

ferner sei $r_,$ irgend eine andere Zahl, für welche

$$r_, R = \alpha_, A + \beta_, B + \dots + i_, I + \lambda_, L + \mu_, M$$

wird.

Bezeichnet $r_{,,}$ den grössten gemeinsamen Theiler von r' und $r_,$, so gibt es zwei Zahlen ρ' und $\rho_,$, welche der Bedingung $\rho' r' - \rho_, r_, = r_{,,}$ genügen, und aus

$$\rho' r' R = \rho' \alpha' A + \rho' \beta' B + \dots + \rho' \lambda' L + \rho' \mu' M$$
$$\rho_, r_, R = \rho_, \alpha_, A + \rho_, \beta_, B + \dots + \rho_, \lambda_, L + \rho_, \mu_, M$$

folgt:

$$\rho' r' R - \rho_, r_, R = r_{,,} R = (\rho' \alpha' - \rho_, \alpha_,) A + \dots + (\rho' \mu' - \rho_, \mu_,) M$$

Da nun r' die kleinste Zahl ist, für welche sich $r' R$ in $A \dots M$ zerlegt, so kann $r_{,,}$ nicht kleiner sein als r', da aber $r_{,,}$ ein Theiler von r' also auch nicht grösser so muss es ihm gleich sein, und daher r' die Zahl $r_,$ theilen, das heisst: *die kleinste Zahl r', für welche die Classe $r' R$ in $A \dots M$ zerlegbar ist, ist ein Theiler jeder andern Zahl $r_,$, für welche $r_, R$ in $A \dots M$ zerlegbar wird.*

Aus dem so eben aufgestellten Satze ergeben sich als specielle Fälle, dass, wenn r'', r''' . . die kleinsten Zahlen sind, für welche

$$r''R = \alpha''A + \quad . \quad . \quad . \quad + i''I + \lambda''L$$
$$r'''R = \alpha'''A + \quad . \quad . \quad . \quad + i'''I$$

wird, r'' durch r' und r''' durch r'' u. s. f. theilbar sein muss.

Sind r'', s'' die kleinsten Zahlen, für welche die Classen $r''R$, $s''S$, in A, B . . I, L zerlegt werden können, so folgt, dass, wenn jetzt ρ'', σ'' die grössten Zahlen bezeichnen, die unter sich relativ prim sind und beziehungsweise die Zahlen r'', s'' theilen, und ferner t'' die kleinste durch r'' und s'' theilbare Zahl bezeichnet also $t'' = \rho''\sigma''$ ist, dann t'' für die Classe $T = \frac{r''}{\rho''}R + \frac{s''}{\sigma''}S$ die kleinste Zahl ist, welche $t''\,T$ in A, B, . . L zerlegbar macht. Die betreffende kleinste Zahl τ muss nemlich, da $\tau\rho''\,T$ und $\tau\rho''\frac{r''}{\rho''}R$ in A, B . . L zerlegbar sind, so beschaffen sein, dass auch $\tau\rho''\frac{s''}{\sigma''}S$ in A . . L zerlegbar ist, also dass nach Obigem $\tau''\rho''\frac{s''}{\sigma''}$ durch s'' theilbar d. h. $\frac{\tau\rho''}{\sigma''}$ eine ganze Zahl wird; ebenso folgt, dass $\frac{\tau\sigma''}{\rho''}$ und demnach $\frac{\tau}{\sigma''\rho''}$ eine ganze Zahl sein muss. Da $\rho'\,\sigma''\,T$ in A. B . . L zerlegbar ist, muss noch $\frac{\rho''\sigma''}{\tau}$ eine ganze Zahl also $\tau = \rho''\sigma''$ sein.

Umfassen also R, S . . *alle zusammengehörigen Classen, sind* r'', s'' . . *die kleinsten Zahlen, für welche* $r''R$, $s''S$, *u. f. in* A, B . . . L *zerlegt werden können und ist unter denselben* r'' *die grösste oder eine der gleichen grössten, so folgt* aus dem eben Bewiesenen, *dass* r'' *durch* s'' . . *u. f. theilbar sein muss.*

5.

Nach der in Art. 3 gemachten Voraussetzung müssen die bei der Darstellung von $r''R$ durch die Classen A, B, . . L auftretenden Anzahlen α'', β'', . . λ'' der von diesen Classen vorkommenden Compositionen durch r'' theilbar sein. Die Classe

$$\frac{\alpha''}{r''}A + \frac{\beta''}{r''}B + \, . \, . + \frac{i''}{r''}I + \frac{\lambda''}{r''}L - R$$

besitzt die Periodenzahl r'', keine Composition dieser Classe mit geringerem Index als r'' ist in $A, B, \ldots I, L,$ zerlegbar und nach dem vorhergehenden Art. hat jede andere Classe, in deren Periode die Haupt-Classe die erste ist, welche in $A, B, \ldots L$ zerlegbar wird, eine Periodenzahl, die ein Theiler von r'' ist. Da nun M eine derartige Classe ist, für welche die Periodenzahl m am grössten wird, so ist $m = r''$ und also m durch $r'', s'', \ldots r', s', \ldots$ theilbar. Ebenso folgt, *dass alle Periodenzahlen $a, b, \ldots l, m$ theilbar sind durch jede Zahl, die angibt, die wie vielste Composition irgend einer Classe zunächst darstellbar wird durch $A, B, \ldots L, M$.*

6.

Bei Benutzung der gebrauchten Bezeichnungen ist

$$\frac{r''}{r'} r' R = \frac{r''}{r'} \alpha' A + \ldots + \frac{r''}{r'} \lambda' L + \frac{r''}{r'} \mu' M$$

und

$$\frac{r''}{r'} r' R - r'' R = \left(\frac{r''}{r'} \alpha' - \alpha''\right) A + \ldots \left(\frac{r''}{r'} \lambda' - \lambda''\right) L + \frac{r''}{r'} \mu' M$$

also

$$\left(m - \frac{r''}{r'} \mu'\right) M = \left(\frac{r''}{r'} \alpha' - \alpha''\right) A + \ldots + \left(\frac{r''}{r'} \lambda' - \lambda''\right) L$$

Diese Darstellung einer Composition von M durch die Classen $A, B, \ldots L$ erfordert nach unseren Voraussetzungen zunächst dass $m - \frac{r''}{r'} \mu'$ durch die Periodenzahl m der Classe M demnach $\frac{r''}{r'} \mu'$ auch durch r'' und also μ' durch r' theilbar sei, ferner dass $\frac{r''}{r'} \lambda' - \lambda''$ durch l also auch durch m und deshalb durch r'' theilbar sei. Da aber auf dieselbe Weise, wie $\frac{\mu'}{r'}$ als ganze Zahl erwiesen ist, auch $\frac{\lambda''}{r''}$ als ganze Zahl folgt, so muss λ' durch r' theilbar sein, die Fortsetzung dieses Verfahrens ergibt, *dass die Zahlen $\alpha', \beta', \ldots \lambda', \mu'$ für die Classe*

$$\alpha' A + \beta' B + \ldots + \lambda' L + \mu' M$$

welche mit der niedrigsten Composition $r' R$ irgend einer Classe R übereinstimmt, durch den Index r' dieser Composition theilbar sind.

7.

Erschöpfen die Classen A, B, . . L, M mit allen ihren Compositionen noch nicht sämmtliche zusammengehörige Classen, so hat man unter den noch übrigen Classen diejenige N' auszuwählen, für welche der Index n der niedrigsten in A, B, . . L, M zerlegbaren Composition nN' unter den Indices aller vorhandenen Classen die grösste oder eine der gleichen grössten Zahlen ist. Wird nun

$$nN' = \alpha A + \beta B + \ldots + \lambda L + \mu M$$

so sind nach dem vorhergehenden Art. $\frac{\alpha}{n}, \frac{\beta}{n}, \ldots \frac{\lambda}{n}, \frac{\mu}{n}$ ganze Zahlen. Die Classe

$$\frac{\alpha}{n} A + \frac{\beta}{n} B + \ldots + \frac{\lambda}{n} L + \frac{\mu}{n} M - N'$$

ist dann eine Classe N, welche die Reihe A, B, . . L, M in der verlangten Weise fortsetzt.

Ihre Periodenzahl ist n, keine Classe in ihrer Periode ausser der Haupt-Classe ist durch Zusammensetzung aus den vorhergehenden Classen darstellbar, weil man sonst eine niedrigere Composition von N' als die n^{te} aufstellen könnte, welche in A, B, . . L, M zerlegbar wäre; auch besitzt sie unter den Classen mit dieser selben Eigenschaft die grösste oder eine der etwa gleichen grössten Periodenzahlen. Aus der Untersuchung in Art. 2 folgt dann, dass keine Classe auf verschiedene Arten durch Zusammensetzung aus A, B, . . L, M, N entstehen kann.

Auf diese Weise lässt sich ein vollständiges System von Fundamental-Classen aufstellen, durch deren Zusammensetzung jede der in Betracht kommenden Classen und zwar jede nur auf Eine bestimmte Art gebildet werden kann.

8.

Aus der Beziehung zwischen den Periodenzahlen der Fundamental-Classen, dass nemlich, wenn sie in der zuvor betrachteten Ordnung aufgestellt sind, jede Periodenzahl durch die Periodenzahl der nachfolgenden

Classe theilbar ist, ergibt sich auch der von Gauss in den Disquiss. Arr. art. 306. VIII angedeutete aber nicht bewiesene Satz über den Zusammenhang zwischen der Anzahl der Classen binärer quadratischer Formen eines Geschlechts und dem Exponenten der Irregularität. Mit diesem Namen bezeichnet Gauss den Quotienten aus der Anzahl der zu einem Geschlechte gehörigen Classen dividirt durch die grösste Periodenzahl, die überhaupt einer Classe des Hauptgeschlechts zukommt.

Die Anzahl der Geschlechter ist nach art. 231 und 287. III der Disquiss. Arr. entweder 1 oder eine Potenz von 2, sie sei 2^{δ}, die einzelnen Geschlechter (der eigentlich primitiven Ordnung) enthalten nach art. 252 gleich viel Classen, die Anzahl sämmtlicher zusammengehöriger Classen ist, wenn $a, b, c \, .\, .\, m, n$ die Periodenzahlen eines vollständigen Systems von Fundamental-Classen bedeuten, gleich $a \,.\, b \,.\, c \,.\,.\, m \,.\, n$, die grösste Periodenzahl für eine Haupt-Classe ist a oder $\frac{a}{2}$, je nachdem ein oder mehre Geschlechter vorhanden sind, weil nach art. 286 jede Classe des Hauptgeschlechts als Duplication bestimmter anderer Classen dargestellt werden kann, demnach ist für den einen oder den anderen Fall der exponens irregularitatis

$$= \frac{abc\ldots mn}{a} \text{ oder } = \frac{abc\ldots mn}{a\,2^{\delta-1}}$$

Ist diese Zahl durch eine ungerade Primzahl p theilbar, so ist die Anzahl der Classen in dem Hauptgeschlecht nemlich

$$abc\ldots mn \quad \text{oder} \quad \frac{abc\ldots mn}{2^{\delta}}$$

durch das Quadrat pp dieser Primzahl theilbar.

Um für die Primzahl 2 den Beweis des entsprechenden Satzes auf ähnliche Art zu führen, hat man ein vollständiges System von Fundamental-Classen zu bilden, welche durch ihre Compositionen nur die Classen des Hauptgeschlechts nemlich jede derselben Ein mal darstellen, was ganz nach den vorhergehenden Untersuchungen auszuführen ist, da die Compositionen von Classen des Hauptgeschlechts mit einander wieder zum Hauptgeschlecht gehören.

9.

Unter den Classen haben diejenigen, welche Formen enthalten, die den ihnen conjugirten äquivalent sind, eine hervorragende Bedeutung durch die Eigenschaften ihrer Compositionen und die enge Beziehung ihrer Anzahl zur Anzahl der Geschlechter. Diese von Gauss Anceps-Classen von Herrn Kummer für die allgemeinen Formen Ambigen genannten Classen ergeben für binäre quadratische (eigentlich primitive) Formen durch Verdoppelung die Haupt-Classe, und jede Classe, deren Composition mit sich selbst die Hauptclasse hervorbringt, ist eine Anceps-Classe, Disquiss. Arr. art. 249. Stellt demnach unter Beibehaltung der im vorhergehenden Artikel gebrauchten Bezeichnung

$$\alpha A + \beta B + \ldots + \mu M + \nu N$$

eine Anceps-Classe dar, so müssen $2\alpha, 2\beta \ldots 2\mu, 2\nu$ der Reihe nach durch $a, b, \ldots m, n$ theilbar sein; umgekehrt: findet dies letztere Statt, so muss jene Classe auch eine Anceps-Classe sein. Bedeutet demnach δ die Anzahl der geraden Periodenzahlen unter $a, b \ldots m, n$, so ist die Anzahl der (eigentlich primitiven) Anceps-Classen, die zu der betreffenden Determinante gehören, $= 2^\delta$.

Ist die Anzahl derjenigen Fundamental-Classen, die nicht dem Hauptgeschlecht angehören, gleich ϑ, so kann ϑ nicht grösser als δ sein, da die Periodenzahl jeder dem Hauptgeschlecht nicht angehörenden Classe gerade ist.

Von den Classen in der Periode irgend einer Classe sind die mit geradzahligem Index in dem Hauptgeschlecht die übrigen in demselben Geschlecht, worin sich die ursprüngliche Classe befindet. Bezeichnet daher θ die Anzahl der Geschlechter mit Ausschluss des Hauptgeschlechts, zu denen die Fundamental-Classen gehören, so übersteigt die Anzahl der Geschlechter, die überhaupt durch Zusammensetzung darstellbare Classen enthalten, nicht 2^θ. Es sollten aber sämmtliche Classen aller Geschlechter hervorgebracht werden, also kann 2^θ nicht kleiner als die Anzahl g der Geschlechter sein. Da nun θ auch nicht das ϑ übertreffen kann, so haben wir die dreifache Beziehung

$$g \leqq 2^\theta \leqq 2^\vartheta \leqq 2^\delta$$

woraus sich wegen der Gleichheit der Anzahl g der Geschlechter und der Anzahl 2^{δ} der Anceps-Classen, Diss. Arr. art. 257, art. 287. III, $\theta = \vartheta = \delta$ ergibt. Hieraus folgt für binäre quadratische eigentlich primitive Formen:

Die Periodenzahlen der Fundamental-Classen aus dem Hauptgeschlecht sind ungerade. Eine Anceps-Classe kann nur durch Compositionen aus den nicht zum Hauptgeschlecht gehörenden Fundamental-Classen entstehen. Bezeichnet δ *die Anzahl der nicht zum Hauptgeschlecht gehörenden Fundamental-Classen, so ist* 2^{δ} *die Anzahl der Anceps-Classen, so wie die Anzahl der Geschlechter.*