Quadratische Körper im Gebiete der höheren Kongruenzen. I.

(Arithmetischer Teil.)

Von

E. Artin in Hamburg.

§ 1.
Einleitung.

Die Dedekindschen Untersuchungen über höhere Kongruenzen[1]) legen folgende Erweiterung der Theorie nahe.

Es werde dem Körper K der rationalen Funktionen modulo p die Funktion $\sqrt{D(t)}$ adjungiert, wo $D(t)$ eine ganze im Sinne Dedekinds quadratfreie Funktion des Parameters t ist. Der entstehende quadratische Körper $K(\sqrt{D(t)})$ weist dann ähnliche Eigenschaften auf wie ein quadratischer Zahlkörper.

So gilt zum Beispiel der Satz über eindeutige Zerlegbarkeit der Ideale in Primideale, der Satz von der Endlichkeit der Klassenzahl, die Sätze über die Einheiten.

Zur Klassenzahlformel gelangt man durch Einführung der Zetafunktionen. Hier läßt sich die Frage nach der Richtigkeit der Riemannschen Vermutung in jedem speziellen Fall entscheiden. Eine Durchrechnung der ersten Fälle — es handelt sich um zirka vierzig Körper — ergab stets die Richtigkeit der Riemannschen Vermutung. Einem allgemeinen Beweis ihrer Richtigkeit scheinen sich aber noch Schwierigkeiten ähnlicher Art wie beim Riemannschen $\zeta(s)$ entgegenzustellen, doch liegen die Verhältnisse hier insofern klarer und durchsichtiger, als es sich (im wesentlichen) um ganze rationale Funktionen handelt. Auf Fragen, die damit im Zusammenhang stehen, werde ich noch zurückkommen.

Von den sonstigen Eigenschaften unserer Zetafunktionen sei noch hervorgehoben: Sie besitzen eine einfache Funktionalgleichung, welche als

[1]) Journ. für die r. u. a. Math. 54 (1857), S. 1—26.

Folge merkwürdige Reziprozitätsbeziehungen gewisser Charaktersummen nach sich zieht. Ihre Nullstellen stehen in einfachem Zusammenhang mit den Wurzeln einer algebraischen Gleichung wodurch eben die Entscheidung über die Riemannsche Vermutung gefällt werden kann.

Setzt man die Richtigkeit der Riemannschen Vermutung für alle Körper voraus, so läßt sich für alle p der Nachweis erbringen, daß es nur endlich viele imaginäre Körper mit einklassigen Geschlechtern gibt.

Endlich sei auch noch auf den Zusammenhang mit einer Arbeit von Kornblum[2]), der am Schlusse des zweiten Teils dieser Arbeit hergestellt wird, hingewiesen. Es gelingt dabei, das Kornblumsche Resultat über die Existenz unendlich vieler Primfunktionen in arithmetischen Progressionen wesentlich zu verschärfen.

Bemerkt sei noch, daß ich der kürzeren Bezeichnung halber einige im Gebiete der Zahlen verwendete Symbole sinngemäß auf die Funktionen (mod p) übertragen habe. Dies rechtfertigt sich auch schon dadurch, daß dann die Analogie unserer Resultate mit denen in Zahlkörpern deutlicher zutage tritt. Eine Verwechslung ist dabei wohl nicht zu befürchten, da die Symbole nur gemäß unserer Definition verwendet werden.

§ 2.

Erste Erweiterung des Rechengebietes.

Nach Dedekind heißen zwei Funktionen $F_1(t) = \sum_{\nu=0}^{n} a_\nu t^\nu$ und $F_2(t) = \sum_{\nu=0}^{n} b_\nu t^\nu$ kongruent modulo p, in Zeichen

$$F_1(t) \equiv F_2(t) \pmod{p},$$

wenn für alle ν gilt

$$a_\nu \equiv b_\nu \pmod{p}.$$

Dabei bedeutet p eine in den ganzen Entwicklungen festgehaltene Primzahl.

Wir wollen in diesem Falle die Funktionen und Zahlen direkt „gleich" nennen und also einfach schreiben

$$F_1(t) = F_2(t), \quad \text{wenn} \quad a_\nu = b_\nu.$$

Von Vielfachen von p ist hierbei eben abgesehen.

Ferner verstehen wir, wenn $a \neq 0$ (d. h. nach der vorigen Festsetzung $a \not\equiv 0 \pmod{p}$), unter $\frac{b}{a}$ eine Zahl x, für welche $ax = b$ ist (d. h. wieder $ax \equiv b \pmod{p}$). Zum Beispiel ist, wenn p ungerade, unter der häufig auftretenden Zahl $\frac{1}{2}$ die ganze Zahl $\frac{p+1}{2}$ zu verstehen.

---

[2]) Mathem. Zeitschr. 5 (1919), S. 100.

Nun lassen wir — und darin besteht unsere Erweiterung — auch negative Potenzen von t in endlicher oder unendlicher Anzahl zu. Wir betrachten also Funktionen der Form

$$F(t) = \sum_{\nu=-\infty}^{n} a_\nu t^\nu = a_n t^n + a_{n-1} t^{n-1} + \ldots \qquad (n \gtrless 0),$$

wobei wieder zwei Funktionen „gleich" sein sollen, wenn die Koeffizienten entsprechender t-Potenzen „gleich" sind.

Man beachte, daß dem Buchstaben t keinerlei numerische Bedeutung zukommt, und er lediglich als Rechensymbol zu betrachten ist, so daß im Falle unendlich vieler negativer Potenzen von t der Konvergenzfrage keinerlei Bedeutung zukommt. Da er ferner im allgemeinen derselbe bleibt, unterdrücken wir künftighin seine Bezeichnung, schreiben also kurz

$$F \quad \text{statt} \quad F(t).$$

Zahlen mögen stets mit kleinen lateinischen Buchstaben und den allgemein üblichen Summationsbuchstaben μ, ν bezeichnet werden, alle übrigen Buchstaben seien den Funktionen vorbehalten.

Sei nun $F = \sum_{\nu=-\infty}^{n} a_\nu t^\nu$, wobei $a_n \neq 0$ vorausgesetzt sei.

F heiße ganz, wenn die Koeffizienten aller negativen Potenzen von t verschwinden, wenn es also eine Funktion im Dedekindschen Sinne ist.

Ferner heiße für ganzes und nicht ganzes F:

1. Wie bei Dedekind, n der Grad von F.

2. Die Zahl p^n der „Betrag" $|F| = p^n$ von F. Diese Bezeichnung wird sich in der Folge rechtfertigen. Für jetzt sei nur bemerkt, daß im Falle eines ganzen F die Zahl $p^n = |F|$ die Anzahl der Restklassen der ganzen Funktionen modulo F ist. In der Dedekindschen Bezeichnung (modd $p, F(t)$). Für von Null verschiedene Zahlen a gilt dann $|a| = 1$. Ferner werde $|0| = 0$ gesetzt.

3. Der Koeffizient a_n der höchsten Potenz von t, der schon bei Dedekind die Rolle des „Vorzeichens" von F spielt, werde mit

$$a_n = \operatorname{sgn} F$$

bezeichnet. Diese Definition hat natürlich nur einen Sinn, wenn $F \neq 0$ ist, d. h. wenn es nichtverschwindende Koeffizienten überhaupt gibt. Dann ist $\operatorname{sgn} F \neq 0$.

4. Mit Dedekind nennen wir die von Null verschiedenen Zahlen $1, 2, \ldots, (p-1)$ die rationalen Einheiten, da sie in *unserem* Sinne ***Teiler*** der Eins sind.

5. Wenn $\operatorname{sgn} F = 1$ ist, heiße F primär. (Es entspricht dies ungefähr den positiven Zahlen.)

Für unsere Symbole gelten nun ersichtlich die gewöhnlichen Rechenregeln:

$$|FG| = |F| \cdot |G|,$$

$\operatorname{sgn}(FG) = \operatorname{sgn} F \cdot \operatorname{sgn} G$.

Wir erwähnen noch die folgenden häufig zur Verwendung gelangenden Regeln:

1. Wenn $|F| < |G|$, so ist

$$|F + G| = |G|.$$

Hier hat ja F auf den Grad des Resultats keinen Einfluß. Ebenso gilt unter der gleichen Voraussetzung

$$\operatorname{sgn}(F + G) = \operatorname{sgn} G.$$

2. Wenn $|F| = |G|$ und $\operatorname{sgn} F + \operatorname{sgn} G \neq 0$ ist, gilt

$$|F + G| = |F| = |G|$$

und

$$\operatorname{sgn}(F + G) = \operatorname{sgn} F + \operatorname{sgn} G.$$

3. Wenn $|F| = |G|$ und $\operatorname{sgn} F + \operatorname{sgn} G = 0$ ist, haben wir

$$|F + G| < |F| = |G|.$$

Der Beweis dieser Sätze folgt unmittelbar aus Gradbetrachtungen.

Das Rechnen mit Grenzwerten erhalten wir durch folgende *Definition*:

Eine Folge von Funktionen $F_1, F_2, F_3, \ldots$ konvergiert gegen einen Grenzwert, in Zeichen $F = \lim_{\nu=\infty} F_\nu$, wenn sich nach Vorgabe eines beliebig kleinen positiven ε ein n so finden läßt, daß für alle $\nu \geqq n$ gilt

$$|F_\nu - F| \leqq \varepsilon.$$

Das heißt ein beliebig gegebener Abschnitt von F kommt von einer Stelle n ab in allen F_ν vor.

Ersichtlich ist hierfür notwendig und hinreichend, wenn eine Stelle n existiert, so daß für $\mu, \nu \geqq n$ gilt

$$|F_\nu - F_\mu| \leqq \varepsilon.$$

Aus dem Grenzwertbegriff folgt unmittelbar der Begriff der Konvergenz und der Summe einer unendlichen Reihe

$$\sum_{\nu=0}^{\infty} F_\nu.$$

Sie konvergiert und hat die Summe S, wenn $S = \lim_{n=\infty} S_n$ existiert, wo

$$S_n = \sum_{\nu=0}^{n} F_\nu.$$

Für die Konvergenz ist notwendig und hinreichend, daß für alle genügend großen μ und $\nu \geqq \mu$ die Beträge der Ausschnitte $F_\mu + F_{\mu+1} + \ldots + F_\nu$ beliebig klein werden.

Da nun einerseits die Beträge dieser Ausschnitte nach unseren Rechenregeln die der einzelnen Glieder nie überschreiten können und andererseits als Ausschnitte für $\mu = \nu$ die einzelnen Glieder selbst auftreten, erhalten wir das einfache Konvergenzkriterium:

Für die Konvergenz der unendlichen Reihe (1) ist notwendig und hinreichend, daß

$$\lim_{\nu=\infty} |F_\nu| = 0.$$

Insbesondere erhalten wir für „Potenzreihen"

$$\sum_{\nu=0}^{\infty} a_\nu F^\nu,$$

deren Koeffizienten Zahlen sind, daß sie sicher konvergieren für

$$|F| \leqq p^{-1}.$$

Denn dann ist:

$$|a_\nu F^\nu| \leqq p^{-\nu}, \quad \text{also} \quad \lim_{\nu=\infty} |a_\nu F^\nu| = 0.$$

Ebenso leicht erhalten wir die Resultate:

Jede konvergente Reihe konvergiert unbedingt, d. h. ihre Glieder können beliebig vertauscht werden.

Für das Produkt zweier konvergenter Reihen gilt die Cauchysche Produktregel.

Definition. Wenn $G \neq 0$ ist, verstehen wir unter $H = \frac{F}{G}$ eine Funktion, für welche $HG = F$ ist.

Um die Existenz einer solchen Funktion nachzuweisen, sei

$$G = a_n t^n + a_{n-1} t^{n-1} + \ldots = a_n t^n (1 - \Phi),$$

wobei $a_n \neq 0$ vorausgesetzt wird. Hier ist

$$\Phi = -\frac{a_{n-1}}{a_n} t^{-1} - \frac{a_{n-2}}{a_n} t^{-2} - \ldots, \quad \text{also} \quad |\Phi| \leqq p^{-1}.$$

Demnach konvergiert

$$\sum_{\nu=0}^{\infty} \Phi^\nu,$$

und es ist

$$(1 - \Phi) \sum_{\nu=0}^{\infty} \Phi^\nu = \sum_{\nu=0}^{\infty} \Phi^\nu - \sum_{\nu=1}^{\infty} \Phi^\nu = 1.$$

Setzen wir also

$$H = a_n^{-1} t^{-n} \cdot F \cdot \sum_{\nu=0}^{\infty} \Phi^\nu,$$

so gilt $HG = F$. Also ist H eine Funktion der gesuchten Art. Aus $AB = 0$ und $A \neq 0$ folgt aber durch Betrachtung der Beträge $B = 0$.

Wäre also H_1 eine zweite Funktion, für die $H_1 G = F$ ist, so wäre $(H - H_1)G = 0$. Wegen $G \neq 0$ folgt $H = H_1$. Also ist $H = \frac{F}{G}$ eindeutig bestimmt.

Aus

$$|F| = |HG| = |H| \cdot |G|$$

folgt die Rechenregel

$$\left|\frac{F}{G}\right| = \frac{|F|}{|G|}$$

und analog ist

$$\operatorname{sgn} \frac{F}{G} = \frac{\operatorname{sgn} F}{\operatorname{sgn} G}.$$

Endlich definieren wir:

Definition. Alle Funktionen, die sich als Quotient zweier ganzer Funktionen darstellen lassen, heißen rational, alle übrigen irrational.

§ 3.

Quadratische Gleichungen und Imaginäre.

Für das Weitere beschränken wir uns auf ungerade Primzahlmoduln p.

Wir untersuchen nun die quadratische Gleichung

$$X^2 = A.$$

Wir erkennen leicht, daß diese Gleichung keine unserem bisherigen Rechengebiete angehörige Lösung haben kann, wenn

1. A ungeraden Grad hat, oder
2. $\operatorname{sgn} A$ quadratischer Nichtrest modulo p ist.

Wenn dagegen A von geradem Grade und $\operatorname{sgn} A = a^2$ ein quadratischer Rest ist, hat unsere Gleichung stets genau zwei nur durch das Vorzeichen verschiedene Lösungen. Denn dann hat A die Form

$$A = a^2 t^{2n} + a_{2n-1} t^{2n-1} + \ldots = a^2 t^{2n}(1 + \Phi),$$

wobei

$$\Phi = \frac{a_{2n-1}}{a^2} t^{-1} + \frac{a_{2n-2}}{a^2} t^{-2} + \ldots, \quad \text{also} \quad |\Phi| \leqq p^{-1}.$$

Nun ist

$$\binom{\frac{1}{2}}{\nu} = \frac{\frac{1}{2} \cdot (-\frac{1}{2}) \ldots (\frac{1}{2} - \nu + 1)}{\nu!} = \frac{(-1)^{\nu-1}}{2^\nu} \frac{1 \cdot 3 \cdot 5 \ldots (2\nu - 3)}{\nu!}$$

oder

$$\binom{\frac{1}{2}}{\nu} = \frac{(-1)^{\nu-1}}{2^{2\nu-1}(\nu-1)} \binom{2\nu-2}{\nu} = \frac{(-1)^{\nu-1}}{2^{2\nu-1}\nu} \cdot \binom{2\nu-2}{\nu-1}.$$

Aus der letzten Gleichheit geht, da $(\nu-1)$ und ν zueinander prim sind, hervor, daß im Nenner von $\binom{\frac{1}{2}}{\nu}$ nur Potenzen von 2 auftreten können. Da wir die Primzahl p als ungerade voraussetzen (der Grund dafür ist das soeben festgestellte Verhalten), können wir $\frac{1}{2}$ durch die ganze Zahl $\frac{p+1}{2}$ ersetzen. Die so entstehende ganze Zahl $\binom{\frac{1}{2}}{\nu}$ gehorcht dann denselben Gesetzen wie das gewöhnliche Symbol, falls nur die Gleichheitszeichen in unserem Sinne als Kongruenzen gelesen werden.

Demnach ist das Quadrat der nach dem Früheren wegen $|\Phi| \leqq p^{-1}$ konvergenten Potenzreihe

$$\sum_{\nu=0}^{\infty} \binom{\frac{1}{2}}{\nu} \Phi^{\nu}$$

(nach der Cauchyschen Regel berechnet) gleich $1+\Phi$, da dies im gewöhnlichen Zahlgebiet der Fall ist.

Die Funktion

$$X = a t^{n} \sum_{\nu=0}^{\infty} \binom{\frac{1}{2}}{\nu} \Phi^{\nu}$$

ist also eine Lösung von $X^2 = \Delta$. Wäre noch $X_1^2 = \Delta$, so hätten wir $X^2 - X_1^2 = 0$ oder $(X+X_1)(X-X_1) = 0$, somit entweder $X = X_1$ oder $X = -X_1$.

Wir schreiben $\sqrt{\Delta} = X$, wo das Vorzeichen noch beliebig wählbar ist, und nennen $\sqrt{\Delta}$ in diesem Falle reell.

Um das Symbol $\sqrt{\Delta}$ auch in den ausgeschlossenen, „imaginären" Fällen zu definieren, gehen wir so vor:

Sei g eine primitive Kongruenzwurzel modulo p, die im weiteren Verlaufe festgehalten werde.

Wir führen nun die beiden „Imaginären" $\sqrt{g}$ und $\sqrt{t}$ ein und betrachten Funktionen der Art:

1. $A + B\sqrt{g}$,
2. $A + B\sqrt{t}$,
3. $A + B\sqrt{gt}$.

Unter Aufrechterhaltung der formalen Rechenregeln für Addition und Multiplikation setzen wir fest, daß $A + B\sqrt{t} = C + D\sqrt{t}$ dann und nur dann zutrifft, wenn $A = C$ und $B = D$ ist. Analog in den übrigen Fällen. Mit den drei Arten werde aber nicht simultan gerechnet. Man überzeugt sich leicht, daß die Aufrechterhaltung der Rechenregeln auf keinen Widerspruch führt, und daß aus dem Verschwinden eines Produktes

auf das Verschwinden eines der Faktoren geschlossen werden darf. In der Tat, wird die Imaginäre mit i bezeichnet, so folgt aus

$$(A + iB)(C + iD) = 0 \quad \text{auch} \quad (A - iB)(C - iD) = 0,$$

also

$$(A^2 - i^2 B^2)(C^2 - i^2 D^2) = 0.$$

Ist nun $A + iB \neq 0$, das heißt verschwinden A und B nicht gleichzeitig, so sind für $i = \sqrt{t}$ oder $i = \sqrt{gt}$ die Grade von A^2 und $i^2 B^2$ sicher verschieden (gerade und ungerade), für $i = \sqrt{g}$ sicher die „Signa". Also ist auch $A^2 - i^2 B^2 \neq 0$. Somit $C^2 - i^2 D^2 = 0$. Nach dem eben Gezeigten geht dies nur, wenn $C = D = 0$, also $C + iD = 0$ ist.

Von der Möglichkeit und Eindeutigkeit der Division überzeugt man sich ebenfalls sofort durch „Rationalmachen" des Nenners.

Für die beiden ausgeschlossenen Fälle ergibt nun eine einfache Betrachtung folgende Möglichkeiten:

$$1.\ \sqrt{\frac{\Delta}{g}} \text{ ist reell} = \sqrt{\Delta_1},$$

$$2.\ \sqrt{\frac{\Delta}{t}} \text{ ist reell} = \sqrt{\Delta_1},$$

$$3.\ \sqrt{\frac{\Delta}{gt}} \text{ ist reell} = \sqrt{\Delta_1}.$$

Es ist hier der Ort darauf hinzuweisen, daß es oft zweckmäßig ist, den Parameter t einer linearen Transformation der Form $t_1 = at + b$ zu unterwerfen. Durch diese wird offenbar keine zahlentheoretische Eigenschaft unserer Funktionen geändert und doch manche Vereinfachung erzielt. So läßt sich zum Beispiel durch $t_1 = gt$ Fall 3 auf Fall 2 zurückführen, so daß es genügte, die Diskussionen für die ersten beiden Fälle durchzuführen. Wir werden gelegentlich von diesen Lineartransformationen Gebrauch zu machen haben.

Die Lösungen von $X^2 = \Delta$ lassen sich also in vier Klassen teilen ($\sqrt{\Delta_1}$ bedeute eine reelle Wurzel):

$$1.\ \sqrt{\Delta} \text{ reell}, \qquad 3.\ \sqrt{\Delta} = \sqrt{t} \cdot \sqrt{\Delta_1},$$

$$2.\ \sqrt{\Delta} = \sqrt{g} \cdot \sqrt{\Delta_1}, \qquad 4.\ \sqrt{\Delta} = \sqrt{gt} \cdot \sqrt{\Delta_1},$$

wobei Fall 3 und 4 nicht wesentlich verschieden sind.

Für die Lösung der quadratischen Gleichung

$$AX^2 + BX + C = 0 \qquad (A \neq 0)$$

ergibt sich nun in bekannter Weise

$$X = \frac{-B \pm \sqrt{B^2 - 4AC}}{2A} = \frac{-B \pm \sqrt{\Delta}}{2A}.$$

§ 4.

Quadratische Körper.

In der zuletzt aufgestellten quadratischen Gleichung mögen nun A, B, C ganze Funktionen sein. Zerlegen wir $\Delta = B^2 - 4AC$ in seine Primfaktoren, so können wir Δ in die Form setzen

$$\Delta = M^2 \cdot D,$$

wo D quadratfrei ist und überdies entweder $\operatorname{sgn} D = 1$ oder $\operatorname{sgn} D = g$. (Indem nämlich ein quadratischer Rest zu M gezogen wird.)

Dann ist $\sqrt{\Delta} = M \cdot \sqrt{D}$. Man erkennt leicht, daß $\sqrt{D}$ nur im Falle $D = 1$, den wir weiterhin als trivial ausschließen, reell und rational ist.

Die Lösung unserer Gleichung hat dann die Form

$$X = \frac{-B \pm M\sqrt{D}}{2A}.$$

Funktionen dieser Form nennen wir quadratische Irrationalitäten und zwar reell oder imaginär, je nachdem $\sqrt{D}$ reell oder imaginär ist.

Die Gesamtheit aller rationalen Funktionen modulo p bildet nun offenbar einen Körper K.

Wir untersuchen nun den Körper Ω, der durch Adjunktion einer quadratischen Irrationalität zu K entsteht. Diese Adjunktion kann offenbar ersetzt werden durch Adjunktion von $\sqrt{D}$. Wir definieren also (Vorzeichen von $\sqrt{D}$ beliebig fest gewählt):

Ist $D \neq 1$ eine ganze quadratfreie Funktion $\bmod p$ und $\operatorname{sgn} D = 1$ oder g, so entsteht der „quadratische Körper" $\Omega = K(\sqrt{D})$ durch Adjunktion von $\sqrt{D}$ zum Körper K. Der Körper heißt reell oder imaginär, je nachdem ob $\sqrt{D}$ reell oder imaginär ist.

Die Funktionen des Körpers $K(\sqrt{D})$ lassen sich darstellen in der Form

$$\alpha = A + B\sqrt{D},$$

wo A und B rational sind.

Sie lassen sich auch nur auf eine Weise so darstellen, denn aus $A + B\sqrt{D} = C + E\sqrt{D}$ würde im Falle $B \neq E$ folgen $\sqrt{D} = \frac{A-C}{E-B}$, so daß $\sqrt{D}$ reell rational wäre. Aus $B = E$ folgt aber wieder $A = C$.

α genügt der Gleichung

$$\alpha^2 - 2A\alpha + (A^2 - DB^2) = 0.$$

Die zweite Wurzel dieser Gleichung

$$\alpha' = A - B\sqrt{D}$$

heißt die zu α konjugierte Funktion. Endlich heißt $\alpha\alpha'$ die Norm von α:

$$N(\alpha) = \alpha\alpha' = A^2 - B^2 D.$$

Definition. Eine Funktion α des Körpers $\Omega = K(\sqrt{D})$ heißt „ganz", wenn sie einer Gleichung

$$\alpha^2 + A_1\alpha + A_2 = 0$$

mit ganz rationalem A_1 und A_2 genügt.

Es gilt der Satz:

Wenn α ganz und rational ist, so ist es ganz rational. Denn aus $\alpha = \frac{F}{G}$, wo F und G prim sind, folgt

$$F^2 + A_1 GF + A_2 G^2 = 0.$$

Also muß F^2 durch G teilbar sein, was nur geht, wenn G eine rationale Einheit ist. Dann ist aber α ganz rational.

Wenn aber α ganz und nicht rational ist, kann es nur einer quadratischen Gleichung der Form

$$\alpha^2 + A_1\alpha + A_2 = 0$$

genügen. Denn aus

$$\alpha^2 + B_1\alpha + B_2 = 0$$

folgte

$$(A_1 - B_1)\alpha + (A_2 - B_2) = 0,$$

was nur für $A_1 = B_1$ richtig sein kann, da sonst α doch rational wäre. Aus $A_1 = B_1$ folgt aber $A_2 = B_2$.

Gehen wir nun auf die Darstellung $\alpha = A + B\sqrt{D}$ und die zugehörige Gleichung

$$\alpha^2 - 2A\alpha + (A^2 - DB^2) = 0$$

zurück, so finden wir, wenn α rational ist, $B = 0$, also A ganz.

Wenn aber α nicht rational ist, muß die hingeschriebene Gleichung, da es dann nur eine dieser Form gibt, ganze rationale Koeffizienten haben. Es ist also $2A$ und demnach A ganz. Ferner ist $A^2 - DB^2$, also auch DB^2 ganz.

Wäre nun B nicht ganz, so bestünde sein Nenner aus mindestens einem Primfaktor, der im Nenner von B^2 quadratisch vorkäme und sich gegen D nicht heben könnte, da D nur einfache Primfaktoren besitzt. Also wäre DB^2 auch nicht ganz.

Ist umgekehrt A und B ganz, so ist ersichtlich $\alpha = A + B\sqrt{D}$ ganz.

Wir haben also:

Satz. Alle ganzen Funktionen des Körpers lassen sich in der Form $\alpha = X + Y\sqrt{D}$ darstellen, wo X und Y ganz sind.

Definition. Jedes Paar ω_1, ω_2 von ganzen Funktionen des Körpers heißt eine Basis, wenn sich alle ganzen Funktionen von Ω in der Form $X\omega_1 + Y\omega_2$ darstellen lassen.

Dann können wir also sagen:

Das Funktionspaar $1, \sqrt{D}$ bildet eine Basis.

Durch ein gleiches Verfahren wie in Zahlkörpern beweist man:

Jede Basis des Körpers hat die Form:

$$\left.\begin{aligned}\omega_1 &= A_1 + A_2\sqrt{D}\\ \omega_2 &= B_1 + B_2\sqrt{D}\end{aligned}\right\}, \quad \text{wo} \quad \begin{vmatrix} A_1 & A_2 \\ B_1 & B_2 \end{vmatrix} = a \text{ ist.}$$

Dabei ist A_1, A_2, B_1, B_2 ganz rational und a eine rationale Einheit.

Aus dem Multiplikationstheorem für Determinanten folgt sofort, wenn ω_1', ω_2' die Konjugierten der Basis ω_1, ω_2 sind:

$$\begin{vmatrix} \omega_1 & \omega_2 \\ \omega_1' & \omega_2' \end{vmatrix}^2 = a_1^2 D_1, \quad \text{wo } a_1 \text{ eine Einheit ist.}$$

Man kann ersichtlich die Basis so wählen, daß a_1^2 ein beliebiger Rest, zum Beispiel 1 wird.

Aus diesem Grunde heißt D die Diskriminante des Körpers $K(\sqrt{D})$.

Aus der Basisdarstellung ergibt sich sofort, das Summe, Differenz und Produkt ganzer Funktionen aus Ω wieder ganz sind, daß mit α auch α' ganz ist, und daß $N(\alpha)$ ganz rational ist.

Definition. Eine ganze Funktion α heißt teilbar durch die ganze Funktion β, wenn sich ein γ (ganz) finden läßt, so daß $\alpha = \beta\gamma$ ist. β heißt auch Teiler von α.

Definition. Jeder Teiler der 1 heißt Einheit des Körpers.

Zu den Einheiten gehören also z. B. die rationalen Einheiten $1, 2, 3, \ldots, (p-1)$, die wir auch triviale Einheiten nennen wollen.

Es gilt der Satz:

Eine ganze Funktion ε ist dann und nur dann Einheit, wenn $N(\varepsilon)$ eine triviale Einheit ist.

Beweis. Aus $N(\varepsilon) = a = \varepsilon\varepsilon'$ folgt $\varepsilon' = \frac{a}{\varepsilon}$. Es ist also $\frac{a}{\varepsilon}$ und somit $\frac{1}{\varepsilon}$ ganz, d. h. ε eine Einheit.

Sei umgekehrt ε eine Einheit und $\varepsilon_1 = \frac{1}{\varepsilon}$, also $\varepsilon\varepsilon_1 = 1$. Dann ist auch $\varepsilon'\varepsilon_1' = 1$, also $N(\varepsilon)\cdot N(\varepsilon_1) = 1$. Die einzigen ganzen rationalen Teiler von 1 sind aber die trivialen Einheiten, so daß $N(\varepsilon) = a$ ist.

Ferner gilt ersichtlich:

Mit ε ist auch $\frac{1}{\varepsilon}$, ε' und $\frac{1}{\varepsilon'}$ eine Einheit.

Das Produkt zweier Einheiten ist selbst eine Einheit.

Definition. Zwei wechselseitig durcheinander teilbare ganze Funktionen α und β heißen assoziiert.

Dann sind also die beiden Quotienten $\frac{\alpha}{\beta}$ und $\frac{\beta}{\alpha}$ ganz, sind also Einheiten. Alle zu α assoziierten Funktionen sind also $\beta = \varepsilon\alpha$, wo ε irgendeine Körpereinheit ist.

Insbesondere sind alle Einheiten untereinander und mit 1 assoziiert.

§ 5.

Die Ideale.

Definition. Ein System ganzer Funktionen von $K(\sqrt{D})$ heißt ein Ideal, wenn mit den Funktionen α_1 und α_2 auch $\gamma_1\alpha_1 + \gamma_2\alpha_2$ zum Ideal gehört, wobei γ_1, γ_2 beliebige Funktionen des Körpers sind.

Satz. In jedem Ideal $\mathfrak{a}$ gibt es eine Basis. Darunter ist ein Funktionspaar ω_1, ω_2 zu verstehen, so daß man durch $X\omega_1 + Y\omega_2$ alle Funktionen des Ideals und nur diese erhält, falls X und Y alle ganzen rationalen Funktionen durchlaufen.

Beweis. Ist α eine Funktion aus $\mathfrak{a}$, so ist auch $\alpha' \cdot \alpha = N(\alpha)$ eine Funktion des Ideals. Im Ideal gibt es also ganze rationale Funktionen. T sei der größte gemeinsame Teiler aller ganz rationalen Funktionen aus $\mathfrak{a}$. Da dieser durch passende lineare Zusammensetzung erhalten werden kann, gehört er selbst dem Ideale an. Ebenso sei $R + S\sqrt{D}$ jene Idealfunktion, für die S der größte gemeinsame Teiler der Koeffizienten von $\sqrt{D}$ in den Idealfunktionen ist. Dann ist

$$\omega_1 = T, \qquad \omega_2 = R + S\sqrt{D}$$

eine Basis des Ideals.

Denn wenn $\alpha = A + B\sqrt{D}$ zu $\mathfrak{a}$ gehört, ist jedenfalls B durch S teilbar: $B = YS$. Mit α gehört auch $\alpha - Y\omega_2 = A - YR$ dem Ideale an. Als ganze rationale Funktion von $\mathfrak{a}$ ist sie durch T teilbar: $\alpha - Y\omega_2 = XT$. Demnach ist

$$\alpha = X\omega_1 + Y\omega_2.$$

Es ist also ω_1, ω_2 eine Basis.

Gleichzeitig haben wir erkannt, daß die Basis stets in der speziellen Form

$$\omega_1 = T, \qquad \omega_2 = R + S\sqrt{D}$$

wählbar ist.

Man erkennt auch leicht, daß $|R| < |T|$ angenommen werden darf. Diese Form der Basis nennen wir die *adaptierte*. T und S sind in ihr

bis auf triviale Einheiten als Faktor eindeutig bestimmt. Nimmt man die Bedingung $|R| < |T|$ hinzu, so ist mit der Wahl von S auch R eindeutig festgelegt. Denn wenn $R + S\sqrt{D}$ und $R_1 + S\sqrt{D}$ dem Ideal angehören mit $|R| < |T|$ und $|R_1| < |T|$, so gehört auch $R - R_1$ dem Ideal an und ist durch T teilbar. Da $|R - R_1| < |T|$ ist, muß $R = R_1$ sein.

Wir beweisen nun den

Satz. Die notwendige und hinreichende Bedingung dafür, daß $\omega = T$, $\omega_2 = R + S\sqrt{D}$ die Basis eines Ideals bildet, lautet: Es muß gelten

$$T = 2CS, \quad R = BS, \quad \frac{B^2 - D}{2C} = 2A,$$

wo A, B, C ganze rationale Funktionen sind. Die Basis hat also die Form

$$\omega_1 = 2CS, \quad \omega_2 = S(B + \sqrt{D}), \quad \text{wo} \quad D = B^2 - 4AC,$$

und umgekehrt ist dann ω_1, ω_2 Basis eines Ideals.

Beweis: 1. Mit $\omega_1 = T$ gehört auch $\omega_1\sqrt{D} = T\sqrt{D}$ zum Ideal, muß sich also durch die Basis darstellen lassen:

$$T\sqrt{D} = \omega_1 X + \omega_2 Y = TX + RY + SY\sqrt{D}.$$

Also:

$$T = SY \quad \text{oder,} \quad Y = 2C \text{ gesetzt,} \quad T = 2CS.$$

Nun muß sein

$$TX + RY = 0,$$

oder nach dem eben gezeigten

$$SYX + RY = 0.$$

Da $T \neq 0$, also $Y \neq 0$ ist, muß sein

$$R = -SX \quad \text{oder,} \quad X = -B \text{ gesetzt,} \quad R = BS.$$

Mit $\omega_2 = S(B + \sqrt{D})$ gehört auch $\omega_2(B - \sqrt{D}) = S(B^2 - D)$ zum Ideal. Es muß durch $T = 2CS$ teilbar sein, also ist $\frac{B^2 - D}{2C}$ ganz. Unsere Bedingungen sind also notwendig.

2. Daß die Bedingungen hinreichen, zeigen wir so. Sei

$$\omega_1 = 2CS, \quad \omega_2 = S(B + \sqrt{D}) \quad \text{und} \quad B^2 - D = 4AC.$$

Die Menge der Funktionen $\gamma_1\omega_1 + \gamma_2\omega_2$, wo γ_1 und γ_2 irgendwelche ganze Funktionen aus $K(\sqrt{D})$ sind, bilden offenbar ein Ideal $\mathfrak{a}$. Jede Zahl α aus $\mathfrak{a}$ hat die Form

$$\begin{aligned}\alpha &= (X + Y\sqrt{D})\,\omega_1 + (X_1 + Y_1\sqrt{D})\,\omega_2 \\ &= S(2CX + BX_1 + Y_1 D) + S(2CY + BY_1 + X_1)\sqrt{D} \\ &= S(2CX + BX_1 + Y_1 D - 2CBY - B^2 Y_1 - BX_1) \\ &\qquad + S(2CY + BY_1 + X_1)\cdot(B + \sqrt{D}) \\ &= 2CS(X - 2AY_1 - BY) + (2CY + BY_1 + X_1)\cdot S(B + \sqrt{D}) \\ &= X_2\omega_1 + Y_2\omega_2,\end{aligned}$$

wo X_2 und Y_2 ganz rational sind. ω_1, ω_2 sind also eine Basis von $\mathfrak{a}$.

Die Basis eines jeden Ideals hat also (wenn sie adaptiert ist) die Form $\omega_1 = 2CS$, $\omega_2 = S\cdot(B + \sqrt{D})$, wo $D = B^2 - 4AC$ ist. C und S sind dabei bis auf triviale Einheitsfaktoren bestimmt. Nimmt man noch $|B| < |C|$ hinzu, so ist auch B vollkommen eindeutig festgelegt.

Satz. Die ganzen rationalen Funktionen A, B, C haben keinen gemeinsamen Teiler.

Es folgt dies aus $D = B^2 - 4AC$ und daraus, daß D keinen quadratischen Teiler hat. Denn einen solchen müßte es geben, wenn ein gemeinsamer Primfaktor von A und C auch in B aufginge.

Wenn ein Ideal $\mathfrak{a}$ aus den Funktionen $\alpha_1, \alpha_2, \ldots, \alpha_n$ so gebildet ist, daß jede Funktion α aus $\mathfrak{a}$ die Form

$$\alpha = \lambda_1\alpha_1 + \lambda_2\alpha_2 + \ldots + \lambda_n\alpha_n \quad (\lambda_\nu \text{ ganze Körperfunktionen})$$

hat, und umgekehrt jede Funktion dieser Form zu $\mathfrak{a}$ gehört, so schreiben wir:

$$\mathfrak{a} = (\alpha_1, \alpha_2, \ldots, \alpha_n).$$

Ersichtlich gilt, wenn ω_1, ω_2 eine Basis ist,

$$\mathfrak{a} = (\omega_1, \omega_2).$$

Jedes Ideal läßt sich also durch höchstens zwei Funktionen aufbauen.

Aus jeder ganzen Funktion α bilden wir das Ideal (α), bestehend aus der Gesamtheit aller durch α teilbaren Funktionen von $K(\sqrt{D})$. Diese Ideale heißen Hauptideale.

Insbesondere ist das System aller ganzen Funktionen des Körpers ein Hauptideal, das Hauptideal (1).

Wir erkennen wieder, daß assoziierte Funktionen und nur diese dasselbe Hauptideal erzeugen. Aus diesem Grunde lassen wir oft bei Hauptidealen die Klammern weg und schreiben kurz α statt (α).

Von den Basen eines Ideals zeigt man leicht:

Satz. Sind ω_1, ω_2 und ω_1^*, ω_2^* zwei Basen des Ideals $\mathfrak{a}$, so ist

$$\left.\begin{aligned}\omega_1^* &= A_1\omega_1 + A_2\omega_2 \\ \omega_2^* &= B_1\omega_1 + B_2\omega_2\end{aligned}\right\} \text{ mit } \begin{vmatrix} A_1 & A_2 \\ B_1 & B_2 \end{vmatrix} = a,$$

wo a eine Einheit ist.

Dies hat zur Folge, daß $\left|\begin{matrix}\omega_1 & \omega_2 \\ \omega_1' & \omega_2'\end{matrix}\right|^2$ bis auf einen quadratischen Rest als Faktor von der Wahl der Basis unabhängig ist und nur vom Ideal abhängt. Die adaptierte Basis ergibt dafür den Wert $(4CS^2)^2 D$. Wir können also setzen

$$\left|\begin{matrix}\omega_1 & \omega_2 \\ \omega_1' & \omega_2'\end{matrix}\right|^2 = a^2 (N\mathfrak{a})^2 \cdot D,$$

wo a^2 ein quadratischer Rest und $N\mathfrak{a}$ ganz rational primär ist.

$N\mathfrak{a}$ heißt die Norm des Ideals $\mathfrak{a}$, ihr Betrag $|N\mathfrak{a}|$ die absolute Norm.

Für $N\mathfrak{a}$ ergibt die adaptierte Basis den Wert

$$N\mathfrak{a} = a_1 \cdot CS^2,$$

wo a_1 eine passende rationale Einheit ist; und zwar wird, da $\operatorname{sgn} N\mathfrak{a} = 1$ ist,

$$N\mathfrak{a} = \frac{CS^2}{\operatorname{sgn} CS^2}.$$

Definition. Sind $\mathfrak{a}$ und $\mathfrak{b}$ zwei Ideale, so ist die Menge der Funktionen $\Sigma\gamma \cdot \alpha\beta$, wo α und β Funktionen von $\mathfrak{a}$ bzw. $\mathfrak{b}$, γ aber beliebige Körperfunktionen sind, ein Ideal $\mathfrak{c}$, welches das Produkt von $\mathfrak{a}$ und $\mathfrak{b}$ genannt werde:

$$\mathfrak{c} = \mathfrak{a}\mathfrak{b}.$$

Es gilt, wie man leicht erkennt,

$$\mathfrak{a}\mathfrak{b} = \mathfrak{b}\mathfrak{a} \quad \text{und} \quad (\mathfrak{a}\mathfrak{b})\mathfrak{c} = \mathfrak{a}(\mathfrak{b}\mathfrak{c}).$$

Für Hauptideale findet man

$$(\alpha)\cdot(\beta) = (\alpha\beta)$$

und

$$(\alpha)\cdot(\beta_1, \beta_2, \ldots, \beta_n) = (\alpha\beta_1, \alpha\beta_2, \ldots, \alpha\beta_n).$$

Also ist

$$\mathfrak{a}\cdot(1) = \mathfrak{a}.$$

Endlich gilt, wenn $\mathfrak{a} = (\alpha_1, \alpha_2)$ und $\mathfrak{b} = (\beta_1, \beta_2)$ ist,

$$\mathfrak{a}\cdot\mathfrak{b} = (\alpha_1\beta_1,\ \alpha_1\beta_2,\ \alpha_2\beta_1,\ \alpha_2\beta_2).$$

Definition. Ersetzt man in einem Ideal $\mathfrak{a}$ alle Funktionen durch ihre Konjugierten, so entsteht wieder ein Ideal $\mathfrak{a}'$, welches das zu $\mathfrak{a}$ konjugierte Ideal genannt werde.

Ist ω_1, ω_2 eine Basis von $\mathfrak{a}$, so ist ω_1', ω_2' eine Basis von $\mathfrak{a}'$.

Das konjugierte Ideal zu $\mathfrak{a}\mathfrak{b}$ ist $\mathfrak{a}'\mathfrak{b}'$.

Endlich: Ist $\mathfrak{a} = (\alpha, \beta)$, so ist $\mathfrak{a}' = (\alpha', \beta')$.

Definition. Ein mit seinem konjugierten identisches Ideal, für welches also $\mathfrak{a} = \mathfrak{a}'$ ist, heißt ambiges Ideal.

Satz. Es ist $\mathfrak{a}\cdot\mathfrak{a}' = (N\mathfrak{a})$ also ein Hauptideal.

Beweis. Sei

$$\omega_1 = 2CS, \quad \omega_2 = S(B+\sqrt{D}), \quad D = B^2 - 4AC$$

die adaptierte Basis von $\mathfrak{a}$. Dann ist:

$$\begin{aligned}\mathfrak{a}\cdot\mathfrak{a}' &= (2CS,\ S(B+\sqrt{D}))\cdot(2CS,\ S(B-\sqrt{D}))\\ &= (S^2)\,(2C,\ B+\sqrt{D})\,(2C,\ B-\sqrt{D})\\ &= (S^2)\,(4C^2,\ 2CB+2C\sqrt{D},\ 2CB-2C\sqrt{D},\ B^2-D)\\ &= (S^2)\,(C^2,\ CB,\ AC,\ C\sqrt{D})\\ &= (C\cdot S^2)\cdot(A,\ B,\ C,\ \sqrt{D}).\end{aligned}$$

Da nun A, B, C keinen gemeinsamen Teiler haben, kommt im letzten Ideal (1) vor. Es ist also

$$\mathfrak{a}\cdot\mathfrak{a}' = (C\cdot S^2)\cdot(1) = (N\mathfrak{a}).$$

Hieraus folgern wir:

Satz. Die Norm des Produktes zweier Ideale ist gleich dem Produkt ihrer Normen. Denn es ist

$$(N(\mathfrak{a}\mathfrak{b})) = (\mathfrak{a}\mathfrak{b})\cdot(\mathfrak{a}\mathfrak{b})' = \mathfrak{a}\mathfrak{a}'\cdot\mathfrak{b}\mathfrak{b}' = (N(\mathfrak{a})\cdot N(\mathfrak{b})).$$

Daher ist $N(\mathfrak{a}\mathfrak{b})$ assoziiert mit $N\mathfrak{a}\cdot N\mathfrak{b}$. Da beide rational und primär sind, gilt also

$$N(\mathfrak{a}\mathfrak{b}) = N\mathfrak{a}\cdot N\mathfrak{b}.$$

Ebenso erhält man:

Satz. Die Norm eines Hauptideals ist, bis auf eine triviale Einheit als Faktor, gleich der Norm der zugehörigen Funktion.

Wie man sieht, laufen die Schlüsse denen im Zahlkörper vollkommen parallel. Es wird also genügen, die weiteren Definitionen und Sätze anzuführen.

Definition. Ist α eine Funktion des Ideals $\mathfrak{a}$, so schreiben wir

$$\alpha \equiv 0 \pmod{\mathfrak{a}}.$$

Ebenso besagt

$$\alpha \equiv \beta \pmod{\mathfrak{a}},$$

daß $\alpha - \beta$ eine Funktion aus $\mathfrak{a}$ ist.

Satz I. Aus $(\gamma)\cdot\mathfrak{a} = (\gamma)\cdot\mathfrak{b}$ folgt $\mathfrak{a} = \mathfrak{b}$.

Satz II. Aus $\mathfrak{a}\cdot\mathfrak{c} = \mathfrak{b}\cdot\mathfrak{c}$ folgt $\mathfrak{a} = \mathfrak{b}$.

Definitionen. 1. Ist $\mathfrak{a} = \mathfrak{b}\mathfrak{c}$, so heißt $\mathfrak{a}$ teilbar durch $\mathfrak{b}$ und $\mathfrak{b}$ ein Teiler von $\mathfrak{a}$.

2. Ein Ideal, welches nur durch (1) und sich selbst teilbar ist, heißt Primideal. (Dabei soll es von (1) verschieden sein.)

Weiter haben wir die Sätze:

III. Ist $\mathfrak{b}$ Teiler von $\mathfrak{a}$ und $\alpha \equiv 0 \pmod{\mathfrak{a}}$, so gilt auch $\alpha \equiv 0 \pmod{\mathfrak{b}}$.

IV. Ein Ideal $\mathfrak{a}$ hat nur endlich viele Teiler.

V. Wenn für jede Funktion β des Ideals $\mathfrak{b}$ gilt $\beta \equiv 0 \pmod{\mathfrak{a}}$, so ist $\mathfrak{b}$ durch $\mathfrak{a}$ teilbar, und umgekehrt. Insbesondere heißt also $\alpha \equiv 0 \pmod{\mathfrak{a}}$: Das Hauptideal (α) ist durch $\mathfrak{a}$ teilbar.

VI. Sind $\mathfrak{a}$ und $\mathfrak{b}$ zwei Ideale, so hat das Ideal $\mathfrak{d}$, welches durch Vereinigung der Funktionen von $\mathfrak{a}$ und $\mathfrak{b}$ gebildet ist, alle Eigenschaften des größten gemeinsamen Teilers von $\mathfrak{a}$ und $\mathfrak{b}$ und ist durch diese eindeutig bestimmt. Es heißt deshalb auch der größte gemeinsame Teiler von $\mathfrak{a}$ und $\mathfrak{b}$: $\mathfrak{d} = (\mathfrak{a}, \mathfrak{b})$.

Wenn $(\mathfrak{a}, \mathfrak{b}) = (1)$ ist, heißen die Ideale $\mathfrak{a}$ und $\mathfrak{b}$ relativ prim. Dann gibt es also aus $\mathfrak{a}$ und $\mathfrak{b}$ je eine Funktion α und β so, daß $\alpha + \beta = 1$ ist.

VII. Wenn das Produkt $\mathfrak{a}\mathfrak{b}$ zweier Ideale durch das Primideal $\mathfrak{p}$ teilbar ist, muß einer der Faktoren durch $\mathfrak{p}$ teilbar sein.

Nunmehr kann der Hauptsatz über die Eindeutigkeit der Zerlegung in Primideale leicht erschlossen werden.

Satz. Jedes Ideal $\mathfrak{a}$ läßt sich auf eine, und bis auf die Anordnung auch nur auf eine Weise in Primideale zerlegen.

Beweis. Wenn $\mathfrak{a}$ nicht selbst Primideal ist, läßt es sich als Produkt zweier Ideale darstellen. Auf diese werde die Betrachtung erneut angewendet. Nach IV muß dies einmal abbrechen, wodurch man die gewünschte Zerlegung erhält:

$$\mathfrak{a} = \mathfrak{p}_1 \mathfrak{p}_2 \dots \mathfrak{p}_n.$$

Aus VII erschließt man die Identität zweier gegebener Zerlegungen.

§ 6.

Primideale.

Satz. Jedes Primideal $\mathfrak{p}$ geht in einer und nur einer rationalen Primfunktion P auf. (Gemeint ist natürlich das Hauptideal (P).)

Beweis. Da $\mathfrak{p}\mathfrak{p}' = N\mathfrak{p}$ ist, erkennen wir, wenn $N\mathfrak{p} = P_1 P_2 \dots P_r$ die Zerlegung von $N\mathfrak{p}$ in Primfunktionen ist, aus $\mathfrak{p}\mathfrak{p}' = P_1 P_2 \dots P_r$, daß $\mathfrak{p}$ in wenigstens einer der Primfunktionen rechterhand aufgeht.

Ist andrerseits $P \equiv 0 \pmod{\mathfrak{p}}$ und $Q \equiv 0 \pmod{\mathfrak{p}}$, wo P und Q verschiedene Primfunktionen sind, so ist auch 1 Funktion von $\mathfrak{p}$, da ja P und Q relativ prim sind. Das geht nicht.

Um alle Primideale zu erhalten, genügt es also alle primären Primfunktionen P zu zerlegen.

Es gehe $\mathfrak{p}$ auf in P:

$$P = \mathfrak{p} \cdot \mathfrak{a},$$

also

$$N(P) = P^2 = N\mathfrak{p} \cdot N\mathfrak{a}.$$

Es kann also nur entweder $N\mathfrak{p} = P$ oder $N\mathfrak{p} = P^2$ sein.

Sei nun $\omega_1 = 2CS$, $\omega_2 = S(B + \sqrt{D})$ eine Basis von $\mathfrak{p}$, wobei C und S primär sind. Dann gilt

$$N\mathfrak{p} = CS^2.$$

1. Die Kongruenz $X^2 \equiv D \pmod{P}$ sei unlösbar. Dann kann C nicht den Wert P haben, da ja für alle $B: (B^2 - D)$ durch P nicht teilbar ist. Wegen $CS^2 = P$ oder P^2 muß also $C = 1$ und $S = P$ sein, also $N\mathfrak{p} = P^2$. Da man $|B| < |C|$ annehmen kann, ist $B = 0$, also

$$\mathfrak{p} = (2P, P\sqrt{D}) = (P) \cdot (1, \sqrt{D}) = (P).$$

P ist also unzerlegbar, somit selbst Primideal.

2. Es sei die Kongruenz $X^2 \equiv D \pmod{P}$ lösbar.

a) P sei prim zu D; B eine Lösung der Kongruenz. Dann ist auch B prim zu P. Wir bilden das Ideal $\mathfrak{p}$ mit der Basis $\omega_1 = P$, $\omega_2 = B + \sqrt{D}$, wo also $S = 1$, $2C = P$ ist. Das geht, da $\frac{B^2 - D}{2C} = \frac{B^2 - D}{P}$ ganz ist. Es ist dann

$$\mathfrak{p} = (P, B + \sqrt{D}), \qquad \mathfrak{p}' = (P, B - \sqrt{D}), \qquad N\mathfrak{p} = P.$$

Wegen $N\mathfrak{p} = P$ ist $\mathfrak{p}$ sicher ein Primideal, und zwar ist $N\mathfrak{p} = \mathfrak{p}\mathfrak{p}' = P$. Ferner ist $\mathfrak{p}$ und $\mathfrak{p}'$ verschieden, denn ihr größter gemeinsamer Teiler ist

$$(P, B + \sqrt{D}, B - \sqrt{D}) = (P, B, \sqrt{D}) = (1).$$

P ist dann also das Produkt zweier verschiedener Primideale $\mathfrak{p}$ und $\mathfrak{p}'$, deren Norm P ist.

b) P sei ein Teiler von D, also $D = PD'$, wo D' prim zu P ist, da D keine quadratischen Teiler enthält. Wir bilden das Ideal $\mathfrak{p}$ mit der Basis $\omega_1 = P$, $\omega_2 = \sqrt{D}$, so daß also $S = 1$, $2C = P$, $B = 0$ ist. Dann ist $\frac{B^2 - D}{2C} = -\frac{D}{P} = D'$ ganz. Wir haben

$$\mathfrak{p} = (P, \sqrt{D}) = \mathfrak{p}', \qquad N\mathfrak{p} = P = \mathfrak{p}\mathfrak{p}' = \mathfrak{p}^2.$$

Es ist also $\mathfrak{p}$ ein Primideal und sein Quadrat gleich P.

Führen wir mit Dedekind das Symbol $\left[\frac{D}{P}\right]$ ein (analog zum Legendreschen, welches $\left(\frac{a}{p}\right)$ geschrieben werde), welches ± 1 sei, je nachdem die Kongruenz $X^2 \equiv D \pmod{P}$ lösbar oder unlösbar ist, und wo D und P relativ prim seien, so haben wir bewiesen:

Satz. 1. Ist P Teiler der Diskriminante D, so ist P das Quadrat eines Primideals

$$P = \mathfrak{p}^2, \quad \text{wo} \quad \mathfrak{p} = (P, \sqrt{D})$$

die Basisdarstellung von $\mathfrak{p}$ ist.

2. Ist P prim zu D und $\left[\frac{D}{P}\right] = +1$, so zerfällt P in das Produkt zweier verschiedener konjugierter Primideale

$$P = \mathfrak{p} \cdot \mathfrak{p}', \quad \text{wo} \quad \mathfrak{p} = (P, B + \sqrt{D}), \quad \mathfrak{p}' = (P, B - \sqrt{D})$$

ihre Basisdarstellung ist, und B eine Wurzel der Kongruenz

$$X^2 \equiv D \pmod{P}.$$

3. Ist P prim zu D und $\left[\frac{D}{P}\right] = -1$, so ist P selbst Primideal und

$$P = (P, P\sqrt{D})$$

seine Basisdarstellung.

Als ambig erkennt man also nur die Primideale der Fälle 1 und 3. Sei nun $\mathfrak{a}$ ein ambiges Ideal $\mathfrak{a} = \mathfrak{a}'$. Mit jedem Primideal $\mathfrak{p}$ geht also auch $\mathfrak{p}'$ in $\mathfrak{a}$ auf. Entweder also geht $\mathfrak{p} \cdot \mathfrak{p}'$ in $\mathfrak{a}$ auf (rationaler Teiler), oder aber $\mathfrak{p}$ ist selbst ambig $\mathfrak{p} = \mathfrak{p}'$. Ziehen wir alle rationalen Teiler zusammen, so erhalten wir also

$$\mathfrak{a} = (A) \cdot \mathfrak{p}_1 \mathfrak{p}_2 \mathfrak{p}_3 \dots \mathfrak{p}_r,$$

wo A ganz rational ist, und $\mathfrak{p}_1, \mathfrak{p}_2, \dots, \mathfrak{p}_r$ verschiedene Primideale des Falles 1 sind. Denn Fall 3 liefert ja rationale Faktoren.

Wir erwähnen noch eine Reihe von Sätzen, deren Beweis man an der Hand der üblichen Beweise leicht konstruieren kann.

Werden nämlich die Funktionen des Körpers in Klassen geteilt, so daß in eine Restklasse alle modulo $\mathfrak{a}$ einander kongruenten Funktionen zu liegen kommen, so gilt:

Satz. Die Anzahl der Restklassen modulo $\mathfrak{a}$, also die Anzahl der einander inkongruenten Funktionen des Körpers, ist gleich der absoluten Norm von $\mathfrak{a}$, also gleich $|N\mathfrak{a}|$.

Faßt man nur die primen Restklassen ins Auge (welche eine Gruppe bilden), so gilt, wenn ihre Anzahl mit $\Phi_D(\mathfrak{a})$ bezeichnet wird:

I. Ist $\mathfrak{a}$ prim zu $\mathfrak{b}$, so ist $\Phi_D(\mathfrak{a}\mathfrak{b}) = \Phi_D(\mathfrak{a}) \cdot \Phi_D(\mathfrak{b})$.

II. Ist $\mathfrak{a} = \mathfrak{p}_1^{n_1} \mathfrak{p}_2^{n_2} \dots \mathfrak{p}_r^{n_r}$ die Zerlegung von $\mathfrak{a}$ in Primideale, so gilt

$$\Phi_D(\mathfrak{a}) = |N\mathfrak{a}| \cdot \left(1 - \frac{1}{|N\mathfrak{p}_1|}\right)\left(1 - \frac{1}{|N\mathfrak{p}_2|}\right) \dots \left(1 - \frac{1}{|N\mathfrak{p}_r|}\right),$$

für Primideale also speziell:

$$\Phi_D(\mathfrak{p}) = |N\mathfrak{p}| - 1.$$

Aus der Gruppeneigenschaft der primen Restklassen folgt der Fermatsche Satz:

III. Ist α prim zu $\mathfrak{a}$, so gilt

$$\alpha^{\Phi_D(\mathfrak{a})} \equiv 1 \pmod{\mathfrak{a}}.$$

Ist also $\mathfrak{a} = \mathfrak{p}$ ein Primideal, so gilt für jede nicht durch $\mathfrak{p}$ teilbare Funktion α

$$\alpha^{|N\mathfrak{p}|-1} \equiv 1 \pmod{\mathfrak{p}}.$$

IV. Eine Kongruenz nach einem Primideal als Modul kann nicht mehr inkongruente Wurzeln haben, als ihr Grad beträgt.

V. Die Anzahl der zum Teiler d von $(|N\mathfrak{p}|-1)$ als Exponent gehörigen primen Restklassen mod $\mathfrak{p}$ ist $\varphi(d)$, wo $\varphi(d)$ die elementare Eulersche Funktion ist.

VI. Die Anzahl der Primitivfunktionen nach einem Primideal $\mathfrak{p}$ beträgt

$$\varphi(|N\mathfrak{p}|-1).$$

§ 7.

Die Idealklassen des Körpers.

Definition. Zwei Ideale $\mathfrak{a}$ und $\mathfrak{b}$ heißen äquivalent, wenn es zwei ganze Funktionen des Körpers, α und β, gibt, so daß

$$(\beta)\cdot\mathfrak{a} = (\alpha)\cdot\mathfrak{b}$$

ist. Wir schreiben:

$$\mathfrak{a} \sim \mathfrak{b}.$$

Die Äquivalenzbeziehung können wir symbolisch auch so ausdrücken:

$$\frac{\mathfrak{a}}{\mathfrak{b}} = \frac{\alpha}{\beta} = \varrho,$$

wo ϱ eine, bis auf eine willkürliche Körpereinheit feste (nicht notwendig ganze) Funktion des Körpers ist. Denn aus $(\beta_1)\mathfrak{a} = (\alpha_1)\mathfrak{b}$ folgt durch Multiplikation mit (β), daß $(\beta_1)(\alpha) = (\alpha_1)(\beta)$ oder $\alpha\beta_1 = \alpha_1\beta\varepsilon$, wo ε eine Einheit ist. Also:

$$\frac{\alpha}{\beta} = \frac{\alpha_1}{\beta_1}\varepsilon.$$

Sofort erkennen wir die Richtigkeit folgender Behauptungen:

1. Aus $\mathfrak{a} \sim \mathfrak{b}$ und $\mathfrak{b} \sim \mathfrak{c}$ folgt $\mathfrak{a} \sim \mathfrak{c}$.
2. Aus $\mathfrak{a} \sim \mathfrak{b}$ und $\mathfrak{c} \sim \mathfrak{d}$ folgt $\mathfrak{a}\mathfrak{c} \sim \mathfrak{b}\mathfrak{d}$.
3. Aus $\mathfrak{a}\mathfrak{c} \sim \mathfrak{b}\mathfrak{d}$ und $\mathfrak{a} \sim \mathfrak{b}$ folgt $\mathfrak{c} \sim \mathfrak{d}$.
4. Aus $\mathfrak{a} \sim \mathfrak{b}$ folgt $\mathfrak{a}' \sim \mathfrak{b}'$.

5. Mit (1) sind die Hauptideale und nur diese äquivalent.

6. Wenn $\frac{\mathfrak{a}}{\mathfrak{b}} = \varrho$ und ω_1, ω_2 eine Basis von $\mathfrak{b}$ ist, so ist $\varrho\omega_1, \varrho\omega_2$ eine Basis von $\mathfrak{a}$.

Beweis. Sei $(\beta)\mathfrak{a} = (\alpha)\mathfrak{b}$ und $\varrho = \frac{\alpha}{\beta}$. β_1 sei eine Funktion aus $\mathfrak{b}$, also $\alpha\beta_1$ eine Funktion aus $(\beta)\mathfrak{a}$. Es ist also $\frac{\alpha\beta_1}{\beta}$ ganz, so daß $\varrho\beta_1$ ganz ist und zwar zu $\mathfrak{a}$ gehört. Also sind $\varrho\omega_1$ und $\varrho\omega_2$ ganz und Funktionen von $\mathfrak{a}$. Also auch jedes $X\cdot(\varrho\omega_1) + Y(\varrho\omega_2)$. Wenn nun α zu $\mathfrak{a}$ gehört, ist $\frac{\alpha}{\varrho}$ ganz und zu $\mathfrak{b}$ gehörig. Also gilt

$$\frac{\alpha}{\varrho} = X\omega_1 + Y\omega_2,$$

somit

$$\alpha = X\cdot\varrho\omega_1 + Y\cdot\varrho\omega_2.$$

Auf Grund von 1 können wir sagen:

Alle untereinander äquivalenten Ideale liegen in einer Klasse, einer Idealklasse $\mathfrak{K}$ des Körpers.

Nach 5 bilden insbesondere die Hauptideale eine Klasse, die Hauptklasse $\mathfrak{K}_0$. In ihr liegt das Ideal (1).

Wegen 2 können wir definieren:

Das Produkt $\mathfrak{K}_1\mathfrak{K}_2$ der beiden Idealklassen $\mathfrak{K}_1$ und $\mathfrak{K}_2$ ist jene Klasse, welche die Produkte der Ideale aus $\mathfrak{K}_1$ mit jener aus $\mathfrak{K}_2$ enthält: $\mathfrak{K}_3 = \mathfrak{K}_1\mathfrak{K}_2$.

Die Multiplikation der Idealklassen ist ersichtlich kommutativ und assoziativ. Für die Hauptklasse $\mathfrak{K}_0$ gilt $\mathfrak{K}\mathfrak{K}_0 = \mathfrak{K}$, wenn $\mathfrak{K}$ irgendeine Klasse ist.

Aus 4 folgt, daß die Ideale, welche zu jenen einer Idealklasse $\mathfrak{K}$ konjugiert sind, auch eine Idealklasse bilden, welche durch einen Akzent gekennzeichnet werde: $\mathfrak{K}'$.

Dann ergibt sich aus $\mathfrak{a}\mathfrak{a}' = (N\mathfrak{a})$, daß $\mathfrak{K}\mathfrak{K}' = \mathfrak{K}_0$, wo $\mathfrak{K}_0$ die Hauptklasse ist.

Punkt 3 kann so geschrieben werden: Aus $\mathfrak{K}_1\mathfrak{K}_2 = \mathfrak{K}_1\mathfrak{K}_3$ folgt $\mathfrak{K}_2 = \mathfrak{K}_3$.

Endlich können wir in der Gleichung $\mathfrak{K}_1\mathfrak{K}_2 = \mathfrak{K}_3$ irgend zwei Klassen beliebig vorschreiben, wodurch dann die dritte eindeutig bestimmt ist.

In der Tat folgt, wenn etwa $\mathfrak{K}_1$ und $\mathfrak{K}_3$ gegeben sind, aus $\mathfrak{K}_1\mathfrak{K}_2 = \mathfrak{K}_3$ durch Multiplikation mit $\mathfrak{K}_1'$:

$$\mathfrak{K}_2 = \mathfrak{K}_1'\mathfrak{K}_3,$$

und umgekehrt ist dann auch

$$\mathfrak{K}_1\mathfrak{K}_2 = \mathfrak{K}_3.$$

Aus dem Bisherigen folgt, daß die Idealklassen eine Abelsche Gruppe bilden.

Dabei ist $\mathfrak{R}_0$ das Einheitselement und $\mathfrak{R}'$ das zu $\mathfrak{R}$ inverse: $\mathfrak{R}^{-1} = \mathfrak{R}'$.

Eine Idealklasse heißt ambig, wenn $\mathfrak{R} = \mathfrak{R}'$ ist (oder $\mathfrak{R} = \mathfrak{R}^{-1}$ oder $\mathfrak{R}^2 = \mathfrak{R}_0$).

Unser nächstes Ziel ist nun, die Endlichkeit der Anzahl der Idealklassen, die wir mit h bezeichnen, nachzuweisen.

§ 8.

Äquivalente Funktionen.

Es sei $\omega = X + Y\sqrt{\Delta}$ (X, Y rational, Δ quadratfrei und $\operatorname{sgn}\Delta = 1$ oder g) eine quadratische Irrationalität. Dann genügen ω und seine Konjugierte $\omega' = X - Y\sqrt{\Delta}$ der Gleichung

$$\omega^2 - 2X\omega + (X^2 - \Delta Y^2) = 0.$$

Setzen wir

$$X^2 - \Delta Y^2 = \frac{A}{C}, \qquad 2X = \frac{B}{C},$$

wo A, B, C ganz und ohne gemeinsamen Teiler seien. Die drei Funktionen sind dann bis auf einen rationalen Einheitsfaktor eindeutig bestimmt. Die Gleichung für ω lautet:

$$C\omega^2 + A = B\omega.$$

Die Diskriminante $B^2 - 4AC$ dieser Gleichung werde nun mit D bezeichnet (D braucht also hier nicht gerade quadratfrei zu sein). D ist dann bis auf einen quadratischen Rest als Faktor festgelegt.

Um nun die Einheitsfaktoren zu normieren, sei zunächst das Vorzeichen von $\sqrt{\Delta}$ so gewählt, daß entweder $\sqrt{\Delta}$ selbst, oder $\frac{1}{\sqrt{g}}\sqrt{\Delta}$, $\frac{1}{\sqrt{t}}\sqrt{\Delta}$, bzw. $\frac{1}{\sqrt{gt}}\sqrt{\Delta}$ primär ist.

Nun findet man leicht $D = 4C^2Y^2\Delta$.

Da Δ quadratfrei ist, muß wieder, wie schon früher einmal, $4C^2Y^2$, also $2CY$ ganz sein.

Der A, B, C gemeinsame willkürliche Einheitsfaktor werde nun so gewählt, daß $\operatorname{sgn}(2CY) = +1$ ist. Dann ist

$$\operatorname{sgn} D = \operatorname{sgn}\Delta.$$

Nun setzen wir noch fest:

$$\sqrt{D} = 2CY \cdot \sqrt{\Delta}, \quad \text{also} \quad Y\sqrt{\Delta} = \frac{\sqrt{D}}{2C}.$$

Auf diese Art sind ω und die Funktionen A, B, C eindeutig aufeinander bezogen. Wir schreiben:

$$\omega = \{A, B, C\} = \frac{B+\sqrt{D}}{2C},$$

wobei zum Beispiel:

$$\omega' = \{-A, -B, -C\} = \frac{B-\sqrt{D}}{2C}.$$

Und zwar ist die Beziehung umkehrbar eindeutig.

Definition. Zwei Funktionen $\omega = \{A, B, C\}$ und $\omega_1 = \{A_1 B_1 C_1\}$ heißen äquivalent, wenn sie miteinander durch eine Beziehung der Form verknüpft sind,

$$\omega_1 = \frac{\alpha\omega+\beta}{\gamma\omega+\delta} \quad \text{mit} \quad \begin{vmatrix} \alpha & \beta \\ \gamma & \delta \end{vmatrix} = a,$$

wo α, β, γ, δ ganz rational sind, und a eine triviale Einheit ist.

Ohne weiteres zeigt man:

Aus $\omega \sim \omega_1$ und $\omega_1 \sim \omega_2$ folgt $\omega \sim \omega_2$.

Aus $\omega \sim \omega_1$ folgt $\omega_1 \sim \omega$.

Durch die Äquivalenzdefinition zerfallen also die Funktionen in Klassen.

Wir haben nun die Transformation der Funktionen A, B, C herzuleiten. Sei

$$\omega = X + Y\sqrt{\Delta}, \qquad \omega_1 = X_1 + Y_1\sqrt{\Delta}.$$

Dann ist

$$X_1 + Y_1\sqrt{\Delta} = \frac{\alpha X+\beta+\alpha Y\sqrt{\Delta}}{\gamma X+\delta+\gamma Y\sqrt{\Delta}},$$

also

$$Y_1 = \frac{-(\alpha X+\beta)\gamma Y+(\gamma X+\delta)\alpha Y}{(\gamma X+\delta)^2-\gamma^2 Y^2\Delta} = \frac{aY}{\gamma^2(X^2-Y^2\Delta)+2X\gamma\delta+\delta^2}.$$

Nach Einführung von A, B, C wird daraus

$$aYC = (A\gamma^2 + B\gamma\delta + C\delta^2)\cdot Y_1. \tag{I}$$

Aus $C\omega^2 + A = B\omega$ erhält man für ω_1 wegen $\omega = \frac{\delta\omega_1-\beta}{-\gamma\omega_1+\alpha}$ die Beziehung

$$C(\delta\omega_1-\beta)^2 + A(-\gamma\omega_1+\alpha)^2 = B(\delta\omega_1-\beta)(-\gamma\omega_1+\alpha)$$

oder

$$\begin{aligned}(A\gamma^2 + B\gamma\delta + C\delta^2)\,\omega_1^2 + (A\alpha^2 + B\alpha\beta + C\beta^2)\\ = (2A\alpha\gamma + B(\alpha\delta+\beta\gamma) + 2C\beta\delta)\,\omega_1.\end{aligned}$$

Vergleicht man dies mit $C_1\omega_1^2 + A_1 = B_1\omega_1$, so erhellt, daß sich die Koeffizienten der beiden Gleichungen nur um einen Faktor unterscheiden können. Ich behaupte, daß dieser Faktor a ist, daß also

$$\left.\begin{aligned} (1)\quad & aA_1 = A\alpha^2 + B\alpha\beta + C\beta^2, \\ (2)\quad & aB_1 = 2A\alpha\gamma + B(\alpha\delta + \gamma\beta) + 2C\beta\delta, \\ (3)\quad & aC_1 = A\gamma^2 + B\gamma\delta + C\delta^2, \end{aligned}\right\} \alpha\delta - \beta\gamma = a.$$

Denn jedenfalls bestehen Gleichungen der Form (1), (2), (3), wo a eine Funktion ist. Setzt man andererseits $\omega_1 = \frac{\alpha\omega+\beta}{\gamma\omega+\delta}$ in $C_1\omega_1^2 + A_1 = B_1\omega_1$ ein, so erhält man Formeln, die aus (1), (2), (3) jedenfalls hervorgehen, indem A, B, C mit A_1, B_1, C_1 vertauscht werden, α durch δ, δ durch α ersetzt werden, und β, γ das Vorzeichen wechseln. Etwa:

$$\left.\begin{aligned} & bA = A_1\delta^2 - B_1\beta\delta + C_1\beta^2, \\ & bB = -2A_1\gamma\delta + B_1(\alpha\delta + \beta\gamma) - 2C_1\alpha\beta, \\ & bC = A_1\gamma^2 - B_1\alpha\gamma + C_1\alpha^2, \end{aligned}\right\} \text{wo } b \text{ wieder eine ganze Funktion ist.}$$

Das Einsetzen in (1) ergibt nach Multiplikation mit b

$$abA_1 = A_1(\alpha\delta - \beta\gamma)^2, \quad \text{also} \quad ab = (\alpha\delta - \beta\gamma)^2,$$

so daß also a und b Einheiten sein müssen. (I) ergibt, wenn wir vorübergehend $\alpha\delta - \beta\gamma$ mit a' bezeichnen:

$$a'YC = aY_1C_1.$$

Da $\operatorname{sgn}(2YC) = \operatorname{sgn}(2Y_1C_1) = 1$ ist, haben wir $a' = a$, also auch $b = a$. Außer (1), (2), (3) gelten also die Formeln:

$$\left.\begin{aligned} (4)\quad & 2YC = 2Y_1C_1, \\ (5)\quad & aA = A_1\delta^2 - B_1\delta\beta + C_1\beta^2, \\ (6)\quad & aB = -2A_1\gamma\delta + B_1(\alpha\delta + \beta\gamma) - 2C_1\alpha\beta, \\ (7)\quad & aC = A_1\gamma^2 - B_1\alpha\gamma + C_1\alpha^2, \end{aligned}\right\} \alpha\delta - \beta\gamma = a.$$

Sei nun D_1 die Diskriminante von $\omega_1 = X_1 + Y_1\sqrt{\Delta}$. Dann ist

$$D_1 = (2C_1Y_1)^2\Delta.$$

Also wegen (4)

$$D_1 = (2CY)^2\Delta = D = B^2 - 4AC = B_1^2 - 4A_1C_1,$$

somit:

Satz. Äquivalente Funktionen haben die gleiche Diskriminante.

§ 9.

Beziehung zwischen Funktionsklassen und Idealklassen — Identität der Klassenzahlen.

Wir betrachten jetzt nur Funktionen ω mit quadratfreier Diskriminante D und fassen zugleich den Körper $K(\sqrt{D})$ ins Auge.

Sei $\mathfrak{a}$ ein Ideal des Körpers mit der Basis

$$\omega_1 = 2CS, \quad \omega_2 = S(B + \sqrt{D}), \quad D = B^2 - 4AC.$$

Wir setzen

$$\omega = \frac{\omega_2}{\omega_1} = \frac{B+\sqrt{D}}{2C}.$$

Dann ist ω wegen $D = B^2 - 4AC$, da ja A, B, C keinen gemeinsamen Teiler haben, eine quadratische Irrationalität mit der Diskriminante D.

Jede andere Basis von $\mathfrak{a}$ hat die Form

$$\left.\begin{aligned}\omega_1^* &= \delta\omega_1 + \gamma\omega_2\\ \omega_1^* &= \beta\omega_1 + \alpha\omega_2\end{aligned}\right\} \quad \text{mit} \quad \begin{vmatrix}\alpha & \beta\\ \gamma & \delta\end{vmatrix} = a,$$

wo α, β, γ, δ ganz rational sind, und umgekehrt ist jedes Funktionspaar dieser Form eine Basis von $\mathfrak{a}$. Wir bilden

$$\omega^* = \frac{\omega_2^*}{\omega_1^*} = \frac{\alpha\omega+\beta}{\gamma\omega+\delta},$$

so daß also $\omega^* \sim \omega$.

Ordnen wir also jedem Ideal seine Basisquotienten zu, so ist ersichtlich jedem Ideal genau eine Klasse äquivalenter Funktionen zugeordnet.

Sei nun $\mathfrak{b}$ ein mit $\mathfrak{a}$ äquivalentes Ideal: $\mathfrak{b} = \varrho\mathfrak{a}$. Wenn ω_1^*, ω_2^* eine Basis von $\mathfrak{a}$ ist, ist $\varrho\omega_1^*$, $\varrho\omega_2^*$ eine Basis von $\mathfrak{b}$, und umgekehrt.

Dem Ideal $\mathfrak{b}$ sind also zuzuordnen seine Basisquotienten $\frac{\varrho\omega_2^*}{\varrho\omega_1^*} = \frac{\omega_2^*}{\omega_1^*} \sim \omega$. Dem Ideal $\mathfrak{b}$ ist also genau die gleiche Funktionsklasse zugeordnet. Es kann ferner die Basis stets so gewählt werden, daß eine beliebige Funktion der Funktionsklasse entsteht.

Es möge nun umgekehrt $\mathfrak{a}$ und $\mathfrak{b}$ der gleichen Funktionsklasse zugeordnet sein. Wir wählen in $\mathfrak{a}$ und $\mathfrak{b}$ je eine Basis ω_1, ω_2 bzw. ω_1^*, ω_2^* derart, daß durch die Basisquotienten die gleiche Funktion entsteht: dies geht nach dem eben Gesagten. Es ist also $\frac{\omega_2}{\omega_1} = \frac{\omega_2^*}{\omega_1^*}$. Also gilt

$$\omega_1^* = \varrho\omega_1, \qquad \omega_2^* = \varrho\omega_2.$$

Dann ist ersichtlich $\mathfrak{b} = \varrho\mathfrak{a}$, da ϱ eine Funktion des Körpers ist.

Es ist also jeder Idealklasse genau eine Funktionsklasse zugeordnet und verschiedenen Idealklassen verschiedene Funktionsklassen.

Es entsteht aber auch jede Funktionsklasse der Diskriminante D. Denn gehört ihr etwa $\omega = \frac{B+\sqrt{D}}{2C}$ mit $D = B^2 - 4AC$ an, so ist $\omega_2 = B + \sqrt{D}$, $\omega_1 = 2C$ die Basis eines Ideals $\mathfrak{a}$, dem der Basisquotient $\frac{\omega_2}{\omega_1}$ zuzuordnen ist.

Es ist also eine ein-eindeutige Zuordnung zwischen den Idealklassen des Körpers $K(\sqrt{D})$ und den Funktionsklassen der Diskriminante D erreicht.

Ist also die Klassenzahl der Funktionsklassen der Diskriminante D endlich, so ist es auch die der Idealklassen, und ihre Anzahl stimmt überein.

Im weiteren Verlaufe wollen wir jedoch die Voraussetzung, daß D quadratfrei ist, wieder fallen lassen, da dadurch keine Vereinfachung erreicht wird.

Die Theorie der Einheiten werden wir auf dieser Grundlage gleichzeitig miterledigen.

Wir beginnen mit dem einfacheren Fall des imaginären Körpers.

§ 10.

Die Endlichkeit der Klassenzahl für imaginäre Funktionen.

Wir führen folgende Bezeichnung ein. Sei

$$X = a_n t^n + a_{n-1} t^{n-1} + \ldots + a_1 t + a_0 + a_{-1} t^{-1} + a_{-2} t^{-2} + \ldots$$

und $n \geqq 0$. Dann schreiben wir

$$E(X) = a_n t^n + a_{n-1} t^{n-1} + \ldots + a_0.$$

Im Falle $n < 0$ dagegen sei

$$E(X) = 0.$$

Das Symbol $E(X)$ steht in Analogie zum Symbol „nächst kleinere ganze Zahl".

Definition. Die imaginäre quadratische Irrationalität $\omega = X + Y\sqrt{\Delta}$ heißt reduziert, wenn sie folgenden Bedingungen genügt:

$$|X| < 1, \tag{1}$$

$$|\omega\,\omega'| \geqq 1, \tag{2}$$

$$\operatorname{sgn} 2Y = 1. \tag{3}$$

Bedingung (2) ist wegen (1) vollkommen gleichbedeutend mit

$$|Y^2 \Delta| \geqq 1. \tag{4}$$

Satz. Jede imaginäre quadratische Irrationalität $\omega = X + Y\sqrt{\Delta}$ ist äquivalent mit einer Reduzierten.

Beweis. Die Funktion $\overline{\omega} = \omega - E(X)$ genügt ersichtlich der Bedingung (1). Genügt sie der Bedingung (2) nicht, so setzen wir $\omega_1 = -\frac{1}{\overline{\omega}} = X_1 + Y_1\sqrt{\Delta}$, wo $\overline{\omega} \sim \omega$, $\omega_1 \sim \omega$ ist, und bilden $\overline{\omega}_1 = \omega_1 - E(X_1)$. $\overline{\omega}_1$ genügt wieder (1). Genügt es (2) nicht, so sei wieder $\omega_2 = -\frac{1}{\overline{\omega}} = X_2 + Y_2\sqrt{\Delta}$ und $\overline{\omega}_2 = \omega_2 - E(X_2)$. So fahren wir fort.

Ich behaupte: Die Funktionen $\overline{\omega}_\nu = \omega_\nu - E(X_\nu)$, wobei $\omega_\nu = -\frac{1}{\overline{\omega}_{\nu-1}}$ ist, welche alle der Bedingung (1) genügen und mit ω äquivalent sind, genügen schließlich der Bedingung (2).

Beweis. Wir setzen $R_\nu = \overline{\omega} \cdot \overline{\omega}'_\nu$ (R_ν ist also als Norm rational!). Dann ist

$$R_\nu = \left(-\frac{1}{\omega_{\nu+1}}\right)\left(-\frac{1}{\omega'_{\nu+1}}\right) = \frac{1}{\omega_{\nu+1}\,\omega'_{\nu+1}}, \quad \text{da ja} \quad \omega_{\nu+1} = -\frac{1}{\overline{\omega}_\nu}.$$

Also:

$$R_\nu = \frac{1}{X_{\nu+1}^2 - Y_{\nu+1}^2 \Delta} = \frac{1}{\omega_{\nu+1}\,\omega'_{\nu+1}}.$$

Aus $\overline{\omega}_\nu = -\frac{1}{\omega_{\nu+1}}$ folgt $\omega_\nu = E(X_\nu) - \frac{1}{\omega_{\nu+1}}$, also

$$X_\nu + Y_\nu\sqrt{\Delta} = E(X_\nu) - \frac{\omega'_{\nu+1}}{\omega_{\nu+1}\,\omega'_{\nu+1}} = E(X_\nu) - R_\nu \cdot \omega'_{\nu+1}.$$

Somit:

$$Y_\nu\sqrt{\Delta} = R_\nu\, Y_{\nu+1}\sqrt{\Delta}.$$

Wegen

$$Y_\nu\sqrt{\Delta} = \frac{\sqrt{D}}{2C_\nu},$$

falls $\omega_\nu = \{A_\nu, B_\nu, C_\nu\}$ gesetzt wird, und wobei $D = B_\nu^2 - 4A_\nu C_\nu$ ist (da ja äquivalente Funktionen gleiche Diskriminante haben), finden wir:

$$C_{\nu+1} = R_\nu C_\nu.$$

Solange nun $|R_\nu| < 1$ ist, finden wir

$$|C_{\nu+1}| < |C_\nu|.$$

Da es aber nur endlich viele ganze rationale Funktionen abnehmenden Grades geben kann, und $C_\nu \neq 0$ ist, muß schließlich einmal $|R_\nu| \geqq 1$ sein. Wegen $R_\nu = \overline{\omega}_\nu \overline{\omega}'_\nu$ bedeutet dies: $\overline{\omega}_\nu$ genügt der Bedingung (2). Setzt man nun

$$\overline{\omega}_\nu = \overline{X}_\nu + \overline{Y}_\nu\sqrt{\Delta},$$

so genügt die Funktion

$$\omega^* = \frac{\overline{\omega}_\nu}{2 \operatorname{sgn} \overline{Y}_\nu}$$

allen drei Bedingungen, und es ist $\omega^* \sim \omega$.

Die Reduziertenbedingung für die Funktion A, B, C finden wir, wenn wir in (1), (2), (4) einsetzen $X = \frac{B}{2C}$, $Y\sqrt{\Delta} = \frac{\sqrt{D}}{2C}$. Sie lauten:

$$|B| < |C| \leqq \sqrt{|D|} \quad \text{und} \quad \operatorname{sgn} C = 1.$$

Gleichzeitig muß $D = B^2 - 4AC$ sein, wegen $|B^2| < |D|$ also $|AC| = |D|$ gelten.

Daraus folgt unmittelbar, daß es zu gegebener Diskriminante nur endlich viele reduzierte Funktionen geben kann, daß also die Klassenzahl von Funktionen gegebener Diskriminante endlich ist.

Für quadratische Körper, also quadratfreie Diskriminanten folgt speziell:

Satz. Die Anzahl der Idealklassen im imaginären Körper $K(\sqrt{D})$ ist endlich.

Wir fragen nun, wann zwei reduzierte Funktionen einander äquivalent sind.

Seien $\omega = \{A, B, C\}$ und $\omega_1 = \{A_1, B_1, C_1\}$ zwei äquivalente reduzierte Funktionen:

$$\omega_1 = \frac{\alpha\omega + \beta}{\gamma\omega + \delta}, \qquad \text{wo } \begin{vmatrix} \alpha & \beta \\ \gamma & \delta \end{vmatrix} = a.$$

Dann folgt aus § 8, (3):

$$4aCC_1 = (2C\delta + B\gamma)^2 - D\gamma^2.$$

Wenn nun der Betrag wenigstens einer der Funktionen C und C_1 kleiner ist als $\sqrt{|D|}$, also $|CC_1| < |D|$ ist, so folgt:

$$|(2C\delta + B\gamma)^2 - D\gamma^2| < |D|.$$

Wäre nun $\gamma \neq 0$, so könnten sich, da $\sqrt{D}$ imaginär ist, also D entweder ungeraden Grad hat oder $\operatorname{sgn} D = g$ ist, die höchsten Potenzen linker Hand nie heben, so daß der Betrag der linken Seite $\geqq |D|$ wäre. Also ist $\gamma = 0$. Dies hat $a = \alpha\delta$ zur Folge, so daß also α und δ triviale Einheiten sind. Aus § 8, (2), (3) folgt dann

$$aC_1 = C\delta^2, \qquad aB_1 = B\alpha\delta + 2C\beta\delta,$$

somit wegen $\operatorname{sgn} C = \operatorname{sgn} C_1 = 1$:

$$a = \alpha\delta = \delta^2, \quad \text{also} \quad \alpha = \delta.$$

Wäre nun $\beta \neq 0$, so erhielte man wegen $|B| < |C|$, da aus der ersten Gleichung $|C| = |C_1|$ folgt, $|B_1| \geqq |C| = |C_1|$, was nicht geht. Es ist also $\beta = \gamma = 0$; $\alpha = \delta$. Somit:

$$\omega_1 = \omega.$$

Ist nun der Grad von D ungerade, so ist stets $|C| < |\sqrt{|D|}|$. Dann sind also alle reduzierten Funktionen untereinander nicht äquivalent und ihre Anzahl die Klassenzahl.

Falls aber der Grad von D gerade ist, kann es reduzierte Funktionen mit $|C| = \sqrt{|D|}$ geben. Die Funktionen mit $|C| < \sqrt{|D|}$ sind dann sicher untereinander und zu denen mit $|C| = \sqrt{|D|}$ nicht äquivalent.

Es bleibt also nur noch der Fall

$$|C| = |C_1| = \sqrt{|D|}$$

zu erledigen. Wegen $|AC| = |D|$ ist dann

$$|A| = |A_1| = \sqrt{|D|}$$

Nun leitet man aus § 8, (1), (3) folgende vier Formeln ab;

$$4aAA_1 = (2A\alpha + B\beta)^2 - D\beta^2,$$
$$4aCA_1 = (2C\beta + B\alpha)^2 - D\alpha^2,$$
$$4aAC_1 = (2A\gamma + B\delta)^2 - D\delta^2,$$
$$4aCC_1 = (2C\delta + B\gamma)^2 - D\gamma^2.$$

Die Beträge der linken Seiten sind genau $|D|$. Wenn nun eine einzige der Funktionen $\alpha, \beta, \gamma, \delta$ keine Zahl wäre, so würde dies in mindestens einer Formel auf einen Widerspruch führen. Wäre z. B. $|\beta| \geqq p$, so würden sich rechterhand in der ersten Formel die höchsten Potenzen nicht wegheben können, da ja $\sqrt{D}$ imaginär ist. Der Betrag der rechten Seite wäre also mindestens $|D\beta^2|$, entgegen dem Betrag der linken Seite.

Die Funktionen $\alpha, \beta, \gamma, \delta$ müssen also Zahlen sein.

Nun gehen wir aus von den Relationen § 8, (1), (2), (3), (6). Wir beachten:

$$|C| = |C_1| = |A| = |A_1| = \sqrt{|D|}, \quad |B| < \sqrt{|D|},$$
$$|B_1| < \sqrt{|D|}, \quad \operatorname{sgn} C = \operatorname{sgn} C_1 = 1,$$

sowie:

$$\operatorname{sgn} D = g = \operatorname{sgn}(B^2 - 4AC) = \operatorname{sgn}(-4AC) = -4 \operatorname{sgn} A,$$

so daß also:

$$\operatorname{sgn} A = \operatorname{sgn} A_1 = -\frac{g}{4}$$

ist. Wir vergleichen nun die höchsten Koeffizienten rechts und links. In (2) und (6) müssen sich wegen $|B| < |C|$ die höchsten Koeffizienten rechts heben.

Wir erhalten so die Formeln

$$\left.\begin{aligned} -\tfrac{g}{4}a &= -\tfrac{g}{4}\alpha^2 + \beta^2 \\ 0 &= -\tfrac{g}{4}\alpha\gamma + \beta\delta \\ a &= -\tfrac{g}{4}\gamma^2 + \delta^2 \\ 0 &= -\tfrac{g}{4}\gamma\delta + \alpha\beta \end{aligned}\right\} \alpha\delta - \beta\gamma = a \neq 0.$$

Wenn umgekehrt

$$|A| = |C| = \sqrt{|D|}, \quad |B| < |C|, \quad \operatorname{sgn} C = 1$$

und

$$\operatorname{sgn} A = -\frac{g}{4} \quad \text{mit} \quad D = B^2 - 4AC$$

ist, und die angeschriebenen Relationen erfüllt sind, so folgt aus (1), (2), (3), daß dann

$$|A_1| = |C_1| = \sqrt{|D|}, \quad |B_1| < \sqrt{|D|}, \quad \operatorname{sgn} C_1 = 1 \text{ und } \operatorname{sgn} A_1 = -\frac{g}{4}$$

ist. Daß also auch das transformierte ω_1 reduziert ist. Unsere Relationen sind also sowohl notwendig wie hinreichend.

1. $\alpha = 0$, also $-\beta\gamma = a$: $\beta \neq 0$, $\gamma \neq 0$; $\beta\delta = 0$, also $\delta = 0$. Ferner $a = -\beta\gamma = -\frac{g}{4}\gamma^2$; $\beta = \frac{g}{4}\gamma$. Also $\alpha = \delta = 0$, $\beta = \frac{g}{4}\gamma$, somit $\omega_1 = \frac{g}{4} \cdot \frac{1}{\omega}$.

2. $\delta = 0$, also $-\beta\gamma = a \neq 0$; $\alpha\beta = 0$, also $\alpha = 0$, d. h. Fall 1.

3. $\gamma = 0$, also $\alpha\delta = a \neq 0$; $\beta\delta = 0$; $\delta = 0$, $\alpha\delta = \delta^2$, somit $\alpha = \delta$, somit $\omega_1 = \omega$.

4. $\beta = 0$; $\alpha\delta = a \neq 0$; $\alpha\gamma = 0$, also $\gamma = 0$, also Fall 3.

Wenn also eine unserer Zahlen verschwindet, kann es sich nur entweder um die triviale Äquivalenzbeziehung $\omega = \omega_1$, oder um

$$\omega_1 = \frac{g}{4} \cdot \frac{1}{\omega}$$

handeln.

Unsere vier Zahlen seien also alle von Null verschieden. Aus $\frac{g}{4}\alpha\gamma = \beta\delta$ und $\frac{g}{4}\gamma\delta = \alpha\beta$ folgt durch Division $\alpha^2 = \delta^2$. Wäre nun $\alpha = -\delta$, so hätte man $-\frac{g}{4}\gamma = \beta$. Also

$$a = \alpha\delta - \beta\gamma = -\delta^2 + \frac{g}{4}\gamma^2.$$

Da aber $a = \delta^2 - \frac{g}{4}\gamma^2$ ist, würde $a = -a$, also $a = 0$ folgen, was nicht geht.

Es ist also $\alpha = \delta$ und $\frac{g}{4}\gamma = \beta$. Dann sind aber auch alle unsere Relationen befriedigt und die zugehörige, mit ω äquivalente Funktion ω_1, da wie bereits gesagt, die Relationen notwendig und hinreichend sind, auch reduziert. Da noch eine unserer Zahlen beliebig wählbar ist, wählen wir $\gamma = 4$, so daß $\beta = g$ wird. Die Äquivalenzbeziehung lautet dann:

$$\omega_1 = \frac{\alpha\omega + g}{4\omega + \alpha} \quad (\alpha = 1, 2, 3, \ldots, (p-1)).$$

Lassen wir auch noch $\alpha = 0$ zu, so kommen wir zur bereits gefundenen Äquivalenzbeziehung $\omega_1 = \frac{g}{4} \cdot \frac{1}{\omega}$.

Sei nun $|D| > 1$. (Der Fall $D = g$ soll gleich erledigt werden.)

Dann sind unsere äquivalenten Funktionen auch wirklich voneinander verschieden. Denn

$$\frac{\alpha\omega+g}{4\omega+\alpha}=\frac{\alpha_1\omega+g}{4\omega+\alpha_1}$$

hat zur Folge $(\alpha-\alpha_1)(4\omega^2-g)=0$.

Somit, wenn $\alpha\neq\alpha_1$ ist, $\omega=\frac{1}{2}\sqrt{g}$. Also der ausgeschlossene Fall $D=g$. Aus

$$\omega=\frac{\alpha\omega+g}{4\omega+\alpha}$$

folgt auch $4\omega^2=g$, also $D=g$.

Zusammenfassung. Für imaginäre quadratische Irrationalitäten sind die reduzierten Funktionen:

1. Im Falle ungeraden Grades von D nie untereinander äquivalent. Die Klassenzahl ist also gleich der Anzahl der reduzierten Funktionen.

2. Im Falle geraden Grades von D und $D\neq g$ sind die Funktionen mit $|C|<\sqrt{|D|}$ weder untereinander noch zu denen mit $|C|=\sqrt{|D|}$ äquivalent. Ihre Anzahl sei r.

Die Funktionen mit $|C|=\sqrt{|D|}$ zerfallen in Gruppen von je $(p+1)$ untereinander äquivalenten Funktionen. Ist ω eine Funktion dieser Gruppe, so sind die p übrigen gegeben durch

$$\omega_\alpha=\frac{\alpha\omega+g}{4\omega+\alpha}\qquad(\alpha=0,1,2,\ldots,p-1).$$

Funktionen aus verschiedenen Gruppen sind miteinander nicht äquivalent.

Ist s die Anzahl der reduzierten Funktionen mit $|C|=\sqrt{|D|}$, so ist s stets durch $p+1$ teilbar, und die Klassenzahl ist

$$h=r+\frac{s}{p+1}.$$

3. Im Falle $D=g$ muß $|C|\leqq 1$, also $C=1$ sein. Ferner $|B|<|C|$, also $B=0$. Dies liefert die einzige reduzierte Funktion $\omega=\frac{1}{2}\sqrt{g}$. Die Klassenzahl ist also eins.

Wenn D quadratfrei ist, ordnen wir den reduzierten Funktionen $\omega=\frac{B+\sqrt{D}}{2C}$ das Ideal $\mathfrak{a}$ von $K(\sqrt{D})$ mit der Basisdarstellung $\mathfrak{a}=(2C, B+\sqrt{D})$ zu. Dieses Ideal nennen wir ein „reduziertes Ideal“. Dann gibt es in jeder Idealklasse reduzierte Ideale. Für sie gilt, da $N\mathfrak{a}=C$ ist, $|N\mathfrak{a}|\leqq\sqrt{|D|}$.

Da die adaptierte Basis, wenn $\operatorname{sgn}C=1$ vorgeschrieben ist, durch das Ideal eindeutig bestimmt ist, sind verschiedenen reduzierten Funktionen verschiedene reduzierte Ideale zugeordnet. Nach dem Früheren entsprechen ferner äquivalenten Idealen äquivalente Funktionen und umgekehrt.

Beispiele. 1. $D = g$. Hier haben wir nur das reduzierte Ideal. $\mathfrak{a} = (2, \sqrt{g}) = (1)$. Die Klassenzahl ist also $h = 1$.

2. $D = t + a$. (Der Fall $D = gt + a$ ist nicht wesentlich verschieden.) Es muß $|C| \leqq 1$, also $C = 1$, $B = 0$ sein. Es gibt also nur die reduzierte Funktion $\omega = \frac{1}{2}\sqrt{t+a}$, im Körper nur das reduzierte Ideal $\mathfrak{a} = (2, \sqrt{D}) = (1)$. Wieder ist $h = 1$.

3. D sei quadratisch, $\operatorname{sgn} D = g$; also $|D| = p^2$, so daß $|C| \leqq p$ sein muß. Für $C = 1$, $B = 0$ liefert dies wieder $\omega = \frac{1}{2}\sqrt{D}$.

Hier haben wir aber noch das Vorkommen linearer C zu berücksichtigen. Zu diesem Zwecke denken wir uns in D durch passende Lineartransformation des Adjunktionsbuchstabens t (dies führt auf einen isomorphen Körper) den Koeffizienten von t zum Verschwinden gebracht. Dann kann über die Transformation noch so verfügt werden, daß nach Hinzufügung passend gewählter quadratischer Reste als Faktoren D eine der Formen

$$D = gt^2 - g, \qquad D = gt^2 - 1, \qquad D = gt^2$$

annimmt.

a) $D = g(t^2 - 1)$. Hier wähle man $C = t + 1$, $B = 0$ und erhält die reduzierte Funktion $\omega_1 = \frac{\sqrt{D}}{2(t+1)}$.

b) $D = g(t^2 - g^{-1})$. Es gibt nun sicher eine Zahl b so, daß $b^2 + 1$ Nichtrest wird. (Denn andernfalls gäbe es ja nur Reste.) Für dieses b ist $g^{-1}(b^2 + 1)$ sicher Rest, also $b^2 - D = -g[t^2 - g^{-1}(1 + b^2)]$ sicher keine Primfunktion. $b^2 - D$ hat also sicher einen Linearteiler $t + a$. Nun setzen wir $C = t + a$, $B = b$ und erhalten die reduzierte Funktion $\omega = \frac{b + \sqrt{D}}{2(t+a)}$.

c) $D = gt^2$. Hier ist $D - b^2 = g(t^2 - g^{-1}b^2)$ stets Primfunktion, wenn $b \neq 0$ ist. Nun muß aber, wenn C linear ist, B eine Zahl sein. Soll $D - b^2$ einen Linearteiler C haben, so muß also $B = b = 0$ sein und $C = t$, $A = -\frac{g}{4}t$. Dann ist aber A, B, C nicht teilerfremd. Also gibt es hier keine Reduzierten mit $|C| = p$. Doch kommt dieser Fall für Körper nicht in Betracht, da ja D durch ein Quadrat teilbar ist.

Wenn C linear ist, gibt es für B nur die Möglichkeiten $B = 0, 1, 2, \ldots, p - 1$. Zu jedem B kann es nun höchstens zwei reduzierte Funktionen geben, nämlich die eventuell linearen Teiler von $B^2 - D$. Im ganzen gibt es also höchstens $2p$ Funktionen unserer Art, somit, da ihre Anzahl durch $p + 1$ teilbar sein soll, entweder gar keine oder genau $p + 1$ äquivalente. In den beiden uns allein interessierenden Fällen a) b) tritt, da wir die Existenz einer Reduzierten unserer Art festgestellt haben, das letztere ein.

Wir haben also:

Ist D quadratfrei und quadratisch, so ist die Klassenzahl des imaginären Körpers $K(\sqrt{D})$ stets $h = 2$.

Dann gibt es zwei Arten reduzierter Ideale:

I. Das Hauptideal $\mathfrak{a} = (2, \sqrt{D}) = (1)$.

II. Nichthauptideale der Form $\mathfrak{a} = (t + a, b + \sqrt{D})$, wo $t + a$ ein Teiler von $b^2 - D$ ist (a, b Zahlen). Und zwar gibt es genau $p + 1$ verschiedene miteinander äquivalente.

§ 11.

Die Anzahl der ambigen Klassen.

Satz. Enthält eine ambige Klasse ein ambiges Ideal, so enthält sie auch ein ambiges reduziertes Ideal.

Beweis. Die Klasse $\mathfrak{K}$ enthalte das ambige Ideal $\mathfrak{a}$ mit der Basisdarstellung $\mathfrak{a} = (2CS, (B + \sqrt{D})S) = (S) \cdot (2C, B + \sqrt{D})$. Da $\mathfrak{a}' = (S)(2C, B - \sqrt{D})$ ist, muß $(2C, B + \sqrt{D}) = (2C, B - \sqrt{D})$ sein (da ja $\mathfrak{a} = \mathfrak{a}'$ ist). Nun ist $\mathfrak{a} \sim (2C, B + \sqrt{D})$, so daß wir vom ambigen Ideal $\mathfrak{a} = (2C, B + \sqrt{D})$ ausgehen. In ihm können wir annehmen, es sei $\operatorname{sgn} C = 1$. Dann ist die adaptierte Basis eindeutig bestimmt. Da $\mathfrak{a}' = (2C, B - \sqrt{D}) = (2C, -B + \sqrt{D}) = \mathfrak{a}$ ist, muß also $B = -B$, also $B = 0$ sein. Wegen $D = -4AC$ ist also C ein Teiler von D. (Es wurde natürlich stillschweigend $|B| < |C|$ vorausgesetzt, was wir annehmen dürfen. Denn nur dann ist die adaptierte Basis eindeutig.) Es ist also $\mathfrak{a} = (2C, \sqrt{D})$. Setzen wir $D = CC' \operatorname{sgn} D$, so ist $\operatorname{sgn} C' = 1$ und C und C' relativ prim. Demnach, wenn $\mathfrak{b} = (2C', \sqrt{D})$ gesetzt wird:

$$\mathfrak{a} \cdot \mathfrak{b} = (2C, \sqrt{D})(2C', \sqrt{D}) = (4CC', 2C'\sqrt{D}, 2C\sqrt{D}, D)$$

$$= (D, \sqrt{D}) = (\sqrt{D}).$$

Also ist $\mathfrak{a}\mathfrak{b} = (\sqrt{D})$, somit, wegen $\mathfrak{a} = \mathfrak{a}'$:

$$(N\mathfrak{a}) \cdot \mathfrak{b} = (\sqrt{D})\mathfrak{a} \quad \text{oder} \quad \mathfrak{b} \sim \mathfrak{a}.$$

Ist also $|C| \geqq \sqrt{|D|}$ so ist $|C'| \leqq \sqrt{|D|}$. Eines der Ideale $\mathfrak{a}$ und $\mathfrak{b}$ ist also reduziert. Da $\mathfrak{a} \sim \mathfrak{b}$ ist, gibt es also in $\mathfrak{K}$ ein ambiges reduziertes Ideal, dessen Basisdarstellung dann lautet:

$$\mathfrak{a} = (2C, \sqrt{D}) \quad \text{mit} \quad |C| \leqq \sqrt{|D|}, \quad \text{wo } C \text{ ein Teiler von } D.$$

Durchläuft C diese Teiler, so erhält man alle ambigen reduzierten Ideale. Die mit $|C| < \sqrt{|D|}$ sind nach unseren Ergebnissen sicher untereinander und mit denen mit $|C| = \sqrt{|D|}$ nicht äquivalent. Zwei verschiedene Ideale $\mathfrak{a} = (2C, \sqrt{D})$, $\mathfrak{b} = (2C', \sqrt{D})$, wo C und C' zwei

Funktionen des Betrags $\sqrt{|D|}$ sind und zu den Teilern von D gehören, sind nach dem Früheren dann und nur dann äquivalent, wenn die zugeordneten Funktionen $\omega = \frac{\sqrt{D}}{2C}$, $\omega_1 = \frac{\sqrt{D}}{2C'}$ es sind. Ferner muß die Äquivalenzbeziehung die Form haben

$$\omega_1 = \frac{\alpha\omega + g}{4\omega + \alpha} \qquad (\alpha = 0, 1, 2, \ldots, p-1).$$

Dies liefert

$$\frac{D}{CC'} + \alpha\frac{\sqrt{D}}{2C'} = \alpha\frac{\sqrt{D}}{2C} + g.$$

Somit

$$D = gCC', \qquad \alpha = 0.$$

Es sind also genau zwei reduzierte Ideale einander äquivalent.

Die Anzahl der einander nicht äquivalenten reduzierten Ideale ist also genau die halbe Teilerzahl von D. Denn ist C ein Teiler, und setzen wir $D = CC' \operatorname{sgn} D$, so ist jedem Teiler C mit $|C| < \sqrt{|D|}$ ein anderer mit $|C| > \sqrt{|D|}$ zugeordnet. Die Teiler mit $|C| = \sqrt{|D|}$ liefern aber nur halb so viel Klassen, wie eben gezeigt wurde.

Wenn also:

$D = g^r P_1 P_2 \ldots P_s$ die Zerlegung von D in Primfunktionen ist, so ist die Anzahl der ambigen Idealklassen, welche ambige Ideale enthalten, genau 2^{s-1}.

Sei nun $\mathfrak{K}$ eine ambige Idealklasse ohne ambiges Ideal und $\mathfrak{a}$ ein reduziertes Ideal der Basisdarstellung $\mathfrak{a} = (2C, B + \sqrt{D})$. Dann ist $B \neq 0$, da sonst $\mathfrak{a}$ ambig wäre. Es ist also, da die Basisdarstellung eindeutig ist, $\mathfrak{a}' = (2C, -B + \sqrt{D})$ ein von $\mathfrak{a}$ verschiedenes und zwar ersichtlich gleichfalls reduziertes Ideal. Nun soll $\mathfrak{a} \sim \mathfrak{a}'$ sein. Dies geht nur, wenn $|C| = \sqrt{|D|}$ (nach dem vorigen Paragraphen) und somit der Grad von D gerade ist. Ist der Grad von D ungerade, so gibt es also keine ambigen Klassen ohne ambiges Ideal.

Wenn nun D geraden Grad hat, seien $\omega = \frac{B+\sqrt{D}}{2C}$, $\omega_1 = \frac{-B+\sqrt{D}}{2C}$ die beiden $\mathfrak{a}$ und $\mathfrak{a}'$ zugeordneten Funktionen.

Damit die Klasse $\mathfrak{K}$ ambig ohne ambiges Ideal sei, ist folgendes notwendig und hinreichend:

1. Es muß sein $\mathfrak{a} \sim \mathfrak{a}'$, also $\omega \sim \omega_1$, somit

$$\omega_1 = \frac{\alpha\omega + g}{4\omega + \alpha} \qquad (\alpha = 0, 1, 2, \ldots, p-1),$$

was

$$4\omega\omega_1 + \alpha(\omega_1 - \omega) = g$$

liefert, und schließlich

$$4A + \alpha B + gC = 0,$$

wo $|A| = |C| = \sqrt{|D|}$ und $|B| < |C|$.

2. Es darf die Idealklasse kein ambiges Ideal, also, da jede Klasse mit ambigem Ideal ein ambiges reduziertes enthält, kein ambiges reduziertes Ideal enthalten, dessen Basis $(2C_1, \sqrt{D})$ lautet. Mit ω sind aber äquivalent nur die Reduzierten

$$\frac{\beta\omega+g}{4\omega+\beta} \qquad (\beta = 0, 1, 2, \ldots, p-1),$$

wo sich dann die Funktionen A, B, C nach § 8, (1), (2), (3) transformieren. Dafür ist notwendig und hinreichend, daß in § 8, (2) das transformierte B_1 für alle β von 0 verschieden ist, daß also

$$aB_1 = 8A\beta + B(\beta^2 + 4g) + 2Cg\beta \not\equiv 0.$$

3. Muß $D = B^2 - 4AC$ sein.

Gibt es andrerseits drei Funktionen A, B, C mit $\operatorname{sgn} C = 1$, welche 1. 2. 3. befriedigen, so bilden sie ein Ideal, welches einer ambigen Idealklasse ohne ambiges Ideal angehört. In

$$8A\beta + B(\beta^2 + 4g) + 2Cg\beta \not\equiv 0 \quad \text{für alle } \beta$$

setzen wir nun ein $4A = -\alpha B - gC$ und erhalten

$$B(\beta^2 - 2\alpha\beta + 4g) \not\equiv 0$$

oder, da $B \not\equiv 0$ ist,

$$\beta^2 - 2\alpha\beta + 4g \not\equiv 0$$

oder endlich

$$(\beta - \alpha)^2 \not\equiv \alpha^2 - 4g.$$

Dies muß für jedes β gelten. Dann kann also links jeder Rest stehen, wie auch α gewählt sei. Damit die Relation befriedigt wird, muß also $\alpha^2 - 4g$ Nichtrest werden.

Für wenigstens eines dieser α soll also

$$4A = -\alpha B - gC$$

zugleich mit

$$D = B^2 - 4AC$$

bestehen. Also muß

$$D = B^2 + \alpha BC + gC^2$$

sein oder

$$4gD = (2gC + \alpha B)^2 - (\alpha^2 - 4g)\cdot B^2.$$

Setzt man $D = gD_1$, so wird also die notwendige und hinreichende Bedingung dafür, daß es eine ambige Idealklasse ohne ambiges Ideal gibt, an die Existenz einer Zahl α geknüpft, für die $(\alpha^2 - 4g)$ Nichtrest wird und

$$D_1 = \left(C + \frac{\alpha}{2g}B\right)^2 - (\alpha^2 - 4g)\left(\frac{B}{2g}\right)^2$$

wird.

Wegen $|C| > |B|$ zeigt eine leichte Überlegung, daß dazu notwendig und hinreichend ist, daß D_1 eine Darstellung in der Form

$$D_1 = X^2 - gY^2 \quad \text{mit} \quad |X| > |Y|$$

gestattet. α kann dabei sogar beliebig gewählt werden, nur muß $\alpha^2 - 4g$ Nichtrest werden, was stets geht.

Diese letzte Bedingung ist aber vollständig äquivalent mit der, daß es überhaupt eine Darstellung der Form

$$D_1 = c(X^2 - gY^2)$$

gibt, wo c irgendeine rationale Einheit ist. Denn aus ihr erhalten wir sofort die neuen Darstellungen

$$D_1 = \frac{c}{a^2 - b^2 g}(a^2 - b^2 g)(X^2 - gY^2) = \frac{c}{a^2 - b^2 g}(X_1^2 - gY_1^2),$$

wo

$$X_1 = aX + bgY, \qquad Y_1 = aY + bX$$

ist und a, b irgendwelche nicht gleichzeitig verschwindende Zahlen sind.

Wenn nun $|X| \neq |Y|$ ist, so wird, wenn $a \neq 0$, $b \neq 0$ gewählt wird, eine Darstellung mit $|X_1| = |Y_1|$ erhalten. Wir können also voraussetzen, es sei $|X| = |Y|$.

Da sich dann des Faktors g wegen die höchsten Potenzen sicher nicht wegheben, muß $|D| = |X^2| = |Y^2|$ sein, was wegen $\operatorname{sgn} D_1 = 1$ zu der Relation führt

$$1 = c((\operatorname{sgn} X)^2 - g(\operatorname{sgn} Y)^2).$$

Nun setzen wir $a = c \operatorname{sgn} X$, $b = -c \operatorname{sgn} Y$. Dann heben sich sicher in Y_1 rechterhand die höchsten Potenzen, in X_1 aber nicht, so daß $|X_1| > |Y_1|$ wird. Ferner ist

$$a^2 - b^2 g = c^2((\operatorname{sgn} X)^2 - g(\operatorname{sgn} Y)^2) = c.$$

Wir haben also wirklich eine Darstellung

$$D_1 = X_1^2 - gY_1^2 \quad \text{mit} \quad |X_1| > |Y_1|$$

erhalten.

Da wir nun in § 15 sehen werden, daß D_1 dann und nur dann eine Darstellung der Form $D_1 = c(X^2 - gY^2)$ gestattet, wenn es durch keine Primfunktion ungeraden Gerades teilbar ist, so können wir, wenn wir dies hier vorwegnehmen wollen, unser Ergebnis so aussprechen (ist D von ungeradem Grade, so ist es ja sicher durch eine Primfunktion ungeraden Grades teilbar):

Im imaginären Körper $K(\sqrt{D})$ existiert dann und nur dann eine ambige Idealklasse, welche kein ambiges Ideal enthält, wenn D durch keine Primfunktion ungeraden Grades teilbar ist.

Unsere Entwicklungen gestatten auch die Repräsentanten dieser Klassen zu berechnen.

Hilfssatz. Sei $K(\sqrt{D})$ ein beliebiger Körper (imaginär oder reell), α eine ganze oder gebrochnene Funktion des Körpers, für welche $N(\alpha) = +1$ ist. Dann gibt es eine ganze Funktion β des Körpers, so daß

$$\alpha = \frac{\beta}{\beta'}$$

wird.

Beweis. Sei $N(\alpha) = \alpha\alpha' = +1$. Wir wählen A ganz rational so, daß $\beta = A(1+\alpha)$ ganz wird. Dann ist $\beta' = A(1+\alpha')$ und somit

$$\frac{\beta}{\beta'} = \frac{1+\alpha}{1+\alpha'} = \frac{\alpha(1+\alpha)}{\alpha+\alpha\alpha'} = \frac{\alpha(1+\alpha)}{\alpha+1} = \alpha.$$

Sei jetzt $\mathfrak{K}$ eine beliebige ambige Idealklasse ohne ambiges Ideal und $\mathfrak{a}$ ein Ideal aus $\mathfrak{K}$. Da $\mathfrak{a} \sim \mathfrak{a}'$ ist, können wir setzen $\frac{\mathfrak{a}}{\mathfrak{a}'} = \alpha$, wo α eine bis auf eine Körpereinheit feste, ganze oder gebrochene Funktion ist. Durch Normenbildung geht hervor, daß $N(\alpha) = a$ ist, wo a eine rationale Einheit ist. Durch Hinzufügung einer passenden rationalen Einheit zu α kann erreicht werden, daß $N(\alpha) = 1$ oder $N(\alpha) = g$ wird. Aus $N(\alpha) = 1$ würde folgen, daß ein ganzes β existiert, so daß $\alpha = \frac{\beta'}{\beta}$ ist. Dann wäre $(\beta\mathfrak{a}) = (\beta\mathfrak{a})'$, also $\beta\mathfrak{a}$ ein ambiges Ideal. Da aber nun $\mathfrak{a} \sim \beta\mathfrak{a}$ ist, kann dies nicht zutreffen, da $\mathfrak{K}$ kein ambiges Ideal enthält. Es ist also $N(\alpha) = g$.

Sei jetzt $\mathfrak{K}_1$ eine zweite ambige Klasse ohne ambiges Ideal, der das Ideal $\mathfrak{a}_1$ angehört. Wieder ist:

$$\frac{\mathfrak{a}_1}{\mathfrak{a}_1'} = \alpha_1 \quad \text{mit} \quad N(\alpha_1) = g$$

und somit

$$\frac{\mathfrak{a}\,\mathfrak{a}_1'}{\mathfrak{a}'\mathfrak{a}_1} = \frac{(\mathfrak{a}\,\mathfrak{a}_1')}{(\mathfrak{a}\,\mathfrak{a}_1')'} = \frac{\alpha}{\alpha_1}, \quad \text{wo jetzt} \quad N\left(\frac{\alpha}{\alpha_1}\right) = 1$$

ist. Es gibt also eine ganze Funktion β, so daß $\frac{\alpha}{\alpha_1} = \frac{\beta}{\beta'}$ ist. Also ist

$$\frac{\mathfrak{a}\,\mathfrak{a}_1'}{(\mathfrak{a}\,\mathfrak{a}_1')'} = \frac{\beta}{\beta'} \quad \text{oder} \quad \mathfrak{a}\,\mathfrak{a}_1'\beta' = (\mathfrak{a}\,\mathfrak{a}_1'\beta')'.$$

Da nun $\mathfrak{a}_1' \sim \mathfrak{a}_1$ also $\mathfrak{a}\,\mathfrak{a}_1'\beta' \sim \mathfrak{a}\,\mathfrak{a}_1$ und somit $\mathfrak{a}\,\mathfrak{a}_1'\beta'$ ein Ideal aus $\mathfrak{K}\mathfrak{K}_1$ ist, enthält die Klasse $\mathfrak{K}\mathfrak{K}_1$ ein ambiges Ideal und ist also eine Klasse $\mathfrak{K}_2$ mit ambigen Idealen.

Aus $\mathfrak{K}\mathfrak{K}_1 = \mathfrak{K}_2$ folgt aber wegen $\mathfrak{K}^2 = \mathfrak{K}_0 =$ Hauptklasse: $\mathfrak{K}_1 = \mathfrak{K}\mathfrak{K}_2$, wo $\mathfrak{K}_2$ ambig und mit ambigem Ideal ist.

Ist andrerseits $\mathfrak{K}$ ambig ohne ambiges Ideal, $\mathfrak{K}_2$ ambig mit ambigem Ideal, so wegen $\mathfrak{K}' = \mathfrak{K}$, $\mathfrak{K}_2' = \mathfrak{K}_2$ auch $(\mathfrak{K}\mathfrak{K}_2)' = \mathfrak{K}\mathfrak{K}_2$, also $\mathfrak{K}\mathfrak{K}_2$ ambig.

Enthielte $\mathfrak{K}\mathfrak{K}_2$ ein ambiges Ideal $\mathfrak{a}_1$, so wäre, $\mathfrak{K}\mathfrak{K}_2 = \mathfrak{K}_1$ gesetzt, $\mathfrak{K} = \mathfrak{K}_1\mathfrak{K}_2$. Ist nun $\mathfrak{a}_2$ ein ambiges Ideal von $\mathfrak{K}_2$, so ist $\mathfrak{a}_1\mathfrak{a}_2$ ein ambiges Ideal aus $\mathfrak{K}$. Es muß also $\mathfrak{K}_1 = \mathfrak{K}\mathfrak{K}_2$ ambig ohne ambiges Ideal sein. Aus der Gruppeneigenschaft erhellt noch, daß lauter verschiedene Klassen erhalten werden, wenn in $\mathfrak{K}\mathfrak{K}_2$ der zweite Faktor alle ambigen Klassen mit ambigem Ideal durchläuft.

Alle ambigen Klassen ohne ambiges Ideal erhält man also aus einer von ihnen etwa $\mathfrak{K}$ durch Bildung von $\mathfrak{K}\mathfrak{K}_2$, wo $\mathfrak{K}_2$ alle ambigen Klassen mit ambigem Ideal durchläuft.

Entweder gibt es also überhaupt keine ambigen Klassen ohne ambiges Ideal, oder ihre Anzahl ist genau so groß wie die der Klassen, welche ambige Ideale enthalten.

Daraus folgt:

Satz. Wenn $D = a \cdot P_1 P_2 P_3 \dots P_s$ die Zerlegung von D in Primfunktionen ist, so ist die Anzahl der ambigen Klassen des imaginären Körpers $K(\sqrt{D})$ gleich

$$2^{s-1} \quad \text{oder} \quad 2^s,$$

je nachdem D durch eine Primfunktion ungeraden Grades teilbar ist oder nicht.

Dies ist dann für die Gruppe der Idealklassen die Anzahl der Geschlechter. Für die Klassenzahl gilt in den beiden Fällen die Zerlegung

$$h = 2^{s-1} \cdot f \quad \text{bzw.} \quad h = 2^s \cdot f,$$

wo f ganz ist.

Ungerade kann also die Klassenzahl nur sein, wenn D eine Primfunktion ungeraden Grades ist.

§ 12.

Kettenbrüche.

Sei F eine reelle Funktion, $E(F)$ das in § 10 definierte Symbol.

Definition. Unter der Kettenbruchentwicklung einer Funktion F verstehen wir folgenden Algorithmus:

Wir setzen sukzessive

$$F = E(F) + \frac{1}{F_1}$$

$$F_1 = E(F_1) + \frac{1}{F_2}$$

$$F_2 = E(F_2) + \frac{1}{F_3}$$

$$\dots\dots\dots\dots$$

Dabei soll der Prozeß abbrechen, wenn einmal F_ν ganz ist, also

$$F_\nu = E(F_\nu)$$

wird. Anderenfalls werde er beliebig weit fortgesetzt.

Aus

$$F_{\nu-1} = E(F_{\nu-1}) + \frac{1}{F_\nu}$$

folgt für $\nu \geqq 1$ wegen der Bedeutung des Symbols $E(F)$, daß

$$\left|\frac{1}{F_\nu}\right| \leqq p^{-1}, \quad \text{also} \quad |F_\nu| \geqq p,$$

und demnach auch

$$|E(F_\nu)| \geqq p.$$

Bricht die Entwicklung mit F_n ab, ist also $F_n = E(F_n)$, so erkennen wir sukzessive: F_n ist rational, also auch F_{n-1}, usw. Es ist also F rational.

Sei umgekehrt F rational: $F = \frac{R}{R_0}$, wo R und R_0 ganz rational sind. Der Algorithmus ergibt:

$$\begin{aligned}
F &= E\left(\frac{R}{R_0}\right) + \frac{R_1}{R_0}, && |R_1| < |R_0|,\\
\frac{R_0}{R_1} &= E\left(\frac{R_0}{R_1}\right) + \frac{R_2}{R_1}, && |R_2| < |R_1|,\\
&\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\\
\frac{R_{\nu-1}}{R_\nu} &= E\left(\frac{R_{\nu-1}}{R_\nu}\right) + \frac{R_{\nu+1}}{R_\nu}, && |R_{\nu+1}| < |R_\nu|.
\end{aligned}$$

Da die Grade stets abnehmen, und unsere Funktionen ganz rational sind, muß schließlich einmal $R_{\nu+1} = 0$ sein, also unser Prozeß abbrechen.

Die Kettenbruchentwicklung bricht also dann und nur dann nie ab, wenn F irrational ist.

Wir wollen nun weiterhin F als irrational voraussetzen. Im Algorithmus $F_\nu = E(F_\nu) + \frac{1}{F_{\nu+1}}$ setzen wir zur Abkürzung $E(F_\nu) = A_\nu$. Dann ist also

$$|A_\nu| \geqq p \quad \text{für} \quad \nu \geqq 1,$$

und es ist

$$F = A_0 + \cfrac{1}{A_1 + \cfrac{1}{A_2 + \cdots + \cfrac{1}{A_{n-1} + \cfrac{1}{F_n}}}}.$$

Die Funktion F_n werde Schlußfunktion genannt. Wie beim gewöhnlichen Kettenbruch gilt die Formel

$$F = \frac{P_n F_n + P_{n-1}}{Q_n F_n + Q_{n-1}},$$

wobei P_n und Q_n ganz rational sind und nach den Rekursionen

$$\left.\begin{aligned} P_{n+1} &= P_n A_n + P_{n-1} \\ Q_{n+1} &= Q_n A_n + Q_{n-1} \end{aligned}\right\} \text{ mit } \left\{\begin{aligned} P_0 &= 1; \quad P_1 = A_0 \\ Q_0 &= 0; \quad Q_1 = 1 \end{aligned}\right.$$

berechnet werden. Es ist daher

$$\begin{aligned} Q_2 &= A_1, && \text{also} && |Q_2| = |Q_1 A_1| \geqq p, \\ Q_3 &= Q_2 A_2 + 1, && \text{also} && |Q_3| = |Q_2 A_2| > |Q_2|, \\ Q_4 &= Q_3 A_3 + Q_2, && \text{also} && |Q_4| = |Q_3 A_3| > |Q_2|, \end{aligned}$$

somit durch Induktion:

$$|Q_\nu| = |Q_{\nu-1} A_{\nu-1}|, \quad \text{also} \quad |Q_\nu| = |A_{\nu-1} A_{\nu-2} \dots A_1|.$$

Wegen $|A_\nu| \geqq p$ für $\nu \geqq 1$ finden wir

$$|Q_\nu| \geqq p^{\nu-1} \quad \text{für} \quad \nu \geqq 1.$$

Ferner liefert das Rekursionssystem:

$$P_n Q_{n-1} - Q_n P_{n-1} = (-1)^n.$$

Dies zeigt, daß P_n und Q_n prim sind.

Satz. Bei einem unendlichen Kettenbruch ist die Folge der Näherungsbrüche: $\frac{P_0}{Q_0}, \frac{P_1}{Q_1}, \dots$ konvergent und es ist:

$$\lim_{\nu=\infty} \frac{P_\nu}{Q_\nu} = F.$$

Beweis. Aus

$$F = \frac{P_\nu F_\nu + P_{\nu-1}}{Q_\nu F_\nu + Q_{\nu-1}}$$

folgt

$$F - \frac{P_\nu}{Q_\nu} = \frac{P_{\nu-1} Q_\nu - P_\nu Q_{\nu-1}}{Q_\nu (Q_\nu F_\nu + Q_{\nu-1})} = \frac{(-1)^{\nu-1}}{Q_\nu (Q_\nu F_\nu + Q_{\nu-1})}.$$

Für $\nu \geqq 1$ ist aber $F_\nu = A_\nu + R_\nu$, also, da $|R_\nu| \leqq p^{-1}$ ist,

$$|Q_\nu F_\nu + Q_{\nu-1}| = |Q_\nu A_\nu| = |Q_{\nu+1}|.$$

Also

$$\left| F - \frac{P_\nu}{Q_\nu} \right| = \frac{1}{|Q_\nu Q_{\nu+1}|} \leqq p^{-(2\nu-1)}.$$

Daraus geht unsere Behauptung unmittelbar hervor.

§ 13.

Kettenbruchentwicklung quadratischer Irrationalitäten — Endlichkeit der Klassenzahl.

Definition. Eine reelle quadratische Irrationalität ω heißt reduziert, wenn ihr Betrag größer als eins, der ihrer Konjugierten aber kleiner als eins ist:

$$|\omega'| < 1 < |\omega|.$$

Satz. Jede reelle quadratische Irrationalität ω ist äquivalent mit einer Reduzierten.

Beweis. Wir entwickeln ω in einen Kettenbruch, dessen Schlußzahlen ω_ν seien. Da ω_ν Schlußfunktion ist, gilt

$$\omega_\nu| > 1.$$

Ferner ist

$$\omega = \frac{P_\nu \omega_\nu + P_{\nu-1}}{Q_\nu \omega_\nu + Q_{\nu-1}} \quad \text{mit} \quad \begin{vmatrix} P_\nu & P_{\nu-1} \\ Q_\nu & Q_{\nu-1} \end{vmatrix} = (-1)^\nu,$$

so daß $\omega \sim \omega_\nu$.

Durch Auflösung erhält man

$$\omega_\nu = -\frac{Q_{\nu-1}\omega - P_{\nu-1}}{Q_\nu \omega - P_\nu},$$

also

$$(1) \qquad \omega_\nu' = -\frac{Q_{\nu-1}\omega' - P_{\nu-1}}{Q_\nu \omega' - P_\nu} = -\frac{Q_{\nu-1}}{Q_\nu} \cdot \frac{(\omega'-\omega) + \left(\omega - \frac{P_{\nu-1}}{Q_{\nu-1}}\right)}{(\omega'-\omega) + \left(\omega - \frac{P_\nu}{Q_\nu}\right)}.$$

Setzen wir nun $|\omega' - \omega| = p^r$, so gilt sicher für $\nu \geqq |r| + 2$

$$\left|\omega - \frac{P_{\nu-1}}{Q_{\nu-1}}\right| \leqq p^{-(2\nu-3)} \leqq p^{-(2|r|+1)},$$

$$\left|\omega - \frac{P_\nu}{Q_\nu}\right| \leqq p^{-(2\nu-1)} \leqq p^{-(2|r|+3)},$$

so daß im zweiten Bruch rechterhand (1) Zähler und Nenner den gleichen Betrag haben. Für $\nu \geqq |r| + 2$ gilt also

$$|\omega_\nu'| = \left|\frac{Q_{\nu-1}}{Q_\nu}\right| = \frac{1}{|A_{\nu-1}|} \leqq p^{-1} < 1,$$

was mit $|\omega_\nu| > 1$ zusammen die Reduziertenbedingung ausmacht.

Satz. Ist ω reduziert, und setzen wir $\omega = E(\omega) + \frac{1}{\omega_1}$, so ist auch ω_1 reduziert. Wegen $\omega_1 \sim \omega$ hat ω_1 die gleiche Diskriminante wie ω.

Beweis. Wegen $|\omega - E(\omega)| < 1$ gilt $|\omega_1| > 1$. Da nun $|\omega| > 1$ ist, ist auch $|E(\omega)| > 1$. Wegen $|\omega'| < 1$ ist also

$$|\omega' - E(\omega)| = |E(\omega)| > 1,$$

somit

$$|\omega_1'| = \frac{1}{|\omega' - E(\omega)|} < 1.$$

Also ist ω_1 auch reduziert.

Satz. In der Beziehung $\omega = E(\omega) + \frac{1}{\omega_1}$ seien ω und ω_1 reduziert. Dann ist nach Vorgabe von ω_1 bereits ω eindeutig bestimmt.

Beweis. Wir haben $\omega' = E(\omega) + \frac{1}{\omega_1'}$, wo $|\omega'| < 1$ und $\left|\frac{1}{\omega_1'}\right| > 1$ ist.

Also ist

$$E(\omega) = -E\left(\frac{1}{\omega_1'}\right),$$

somit

$$\omega = -E\left(\frac{1}{\omega_1'}\right) + \frac{1}{\omega_1},$$

womit ω bestimmt ist.

Daraus folgt: Die Schlußfunktionen ω_ν in der Kettenbruchentwicklung einer reellen quadratischen Irrationalität ω sind schließlich reduziert, und mit einer von ihnen sind es auch alle folgenden.

Ist speziell ω reduziert, so sind alle Schlußfunktionen reduziert, und mit einer von ihnen sind nicht nur alle folgenden, sondern auch alle vorhergehenden eindeutig bestimmt.

Für die Funktionen A, B, C lautet wegen

$$\omega = \frac{B+\sqrt{D}}{2C}, \quad \omega' = \frac{B-\sqrt{D}}{2C}$$

die Reduziertenbedingung

$$|B - \sqrt{D}| < |C| < |B + \sqrt{D}|.$$

Wäre nun $|B| \neq |\sqrt{D}|$, so wäre $|B + \sqrt{D}| = |B - \sqrt{D}|$, so daß die Ungleichheitszeichen nicht stehen könnten. Es ist also $|B| = |\sqrt{D}|$. Ferner müssen, da ja beide Ungleichheitszeichen gelten sollen, die Grade von $B - \sqrt{D}$ und $B + \sqrt{D}$ sich also um mindestens zwei Einheiten unterscheiden müssen, die beiden höchsten Potenzen von B und $\sqrt{D}$ übereinstimmen. Dies gibt nur endlich viel Möglichkeiten für B, falls D vorgegeben ist, und unserer Ungleichung halber zu jedem B nur endlich viele C, die noch durch die Bedingung $D = B^2 - 4AC$ eingeschränkt werden.

Es gibt also zu gegebener Diskriminante D nur endlich viele Reduzierte, also ist die Klassenanzahl der Funktionen der Diskriminante D endlich.

Wenn D quadratfrei ist, folgt speziell:

Satz. Im reellen quadratischen Körper $K(\sqrt{D})$ ist die Anzahl der Idealklassen endlich.

Ferner allgemein:

Die Kettenbruchentwicklung einer reduzierten quadratischen Irrationalität und nur einer solchen, ist rein periodisch. Die der übrigen (quadratischen) Irrationalitäten gemischt periodisch.

Beispiel. Der einfachste reelle Körper ist $K(\sqrt{t^2 + a_1 t + a_2})$, wo $a_2 - \frac{1}{4}a_1^2 \neq 0$ sein muß, da sonst D ein volles Quadrat ist. Wir haben $\sqrt{D} = t + \frac{1}{2}a_1 + \ldots$. Da die beiden ersten Potenzen von B und $\sqrt{D}$

übereinstimmen, ist $B = t + \frac{1}{2}a_1$, also $D - B^2 = a_2 - \frac{1}{4}a_1^2 \neq 0$. Also muß C eine Einheit b sein. Die reduzierten Funktionen sind also: $c(t + \frac{1}{2}a_1 + \sqrt{D})$. Sie sind miteinander äquivalent, also ist die Klassenzahl unseres Körpers $h = 1$.

Die Kettenbruchentwicklung der Reduzierten finden wir nach leichter Rechnung $(E(\sqrt{D}) = t + \frac{1}{2}a_1)$ zu:

$$\omega = c(2t + a_1) + c\left(-t - \frac{1}{2}a_1 + \sqrt{D}\right) = c(2t + a_1) + \cfrac{1}{t + \frac{1}{2}a_1 + \sqrt{D}},$$

$$\cfrac{t + \frac{1}{2}a_1 + \sqrt{D}}{c\left(a_2 - \frac{1}{4}a_1^2\right)} = \cfrac{2t + a_1}{c\left(a_2 - \frac{1}{4}a_1^2\right)} + \cfrac{1}{c\left(t + \frac{1}{2}a_1 + \sqrt{D}\right)} = \cfrac{2t + a_1}{c\left(a_2 - \frac{1}{4}a_1^2\right)} + \frac{1}{\omega}.$$

Also haben wir

$$c\left(t + \frac{1}{2}a_1 + \sqrt{D}\right) = c(2t + a_1) + \cfrac{1}{\cfrac{2t + a_1}{c\left(a_2 - \frac{1}{4}a_1^2\right)} + \cfrac{1}{c(2t + a_1) + \cfrac{1}{\cfrac{2t + a_1}{c\left(a_2 - \frac{1}{4}a_1^2\right)} + \ldots}}}.$$

Eine eingliedrige Periode gibt es unter den reduzierten Funktionen also nur, wenn $c = \cfrac{1}{c\left(a_2 - \frac{1}{4}a_1^2\right)}$ oder $a_2 - \frac{1}{4}a_1^2 = \frac{1}{c^2}$ ist. Wenn also $a_2 - \frac{1}{4}a_1^2$ quadratischer Rest ist.

Im Körper $K(\sqrt{D})$ ordnen wir nun wieder den reduzierten Funktionen $\omega = \frac{B + \sqrt{D}}{2C}$ das „reduzierte Ideal“

$$\mathfrak{a} = (2C, B + \sqrt{D})$$

zu. Dann gibt es in jeder Klasse reduzierte Ideale. Es gilt wieder $|N\mathfrak{a}| < |\sqrt{D}|$.

§ 14.

Die Einheiten des quadratischen Körpers.

Die ganze Funktion $\varepsilon = U + V\sqrt{D}$ ist dann und nur dann eine Einheit, wenn $N(\varepsilon) = c$ ist, wo c eine triviale Einheit ist.

Die Bestimmung aller Einheiten ist also äquivalent mit der Auflösung der „Pellschen Gleichung“

$$U^2 - V^2 D = c.$$

I. Der Körper $K(\sqrt{D})$ sei imaginär.

$$D = g, \qquad U^2 - V^2 g = c. \tag{1}$$

Da sich, wenn $|V| > 1$ ist, die höchsten Potenzen nicht wegheben können, muß v eine Zahl b und demnach auch U eine Zahl a sein

Alle Einheiten haben also die Form

$$\varepsilon = a + b\sqrt{g},$$

wo a und b zwei nicht gleichzeitig verschwindende Zahlen sind.

Ihre Anzahl ist also $w = p^2 - 1$.

Ferner ist $N(\varepsilon) = a^2 - b^2 g$ und kann ersichtlich jede triviale Einheit sein. Die Anzahl der Einheiten gegebene Norm ist $p + 1$.

$$|D| \geqq p, \quad U^2 - V^2 D = c. \tag{2}$$

Wäre $V \neq 0$, so könnten sich wieder die höchsten Potenzen nicht heben. Aus $V = 0$ folgt aber, daß U eine triviale Einheit ist. Die trivialen Einheiten sind also hier die einzigen. Ihre Norm muß quadratischer Rest sein, und zu gegebener Norm gibt es zwei nur durch das Vorzeichen verschiedene Einheiten. Die Anzahl der Einheiten ist hier $w = p - 1$.

II. Der Körper $K(\sqrt{D})$ sei reell.

Sei ω eine zur Diskriminante D gehörige reduzierte Funktion. Wir entwickeln ω in einen Kettenbruch mit den Schlußfunktionen $\omega_1, \omega_2, \omega_3, \ldots$. Da er rein periodisch ist, muß unter ihnen schließlich einmal ω wieder auftreten. Sei etwa $\omega_n = \omega$. Dann ist

$$\omega = \frac{P_n \omega + P_{n-1}}{Q_n \omega + Q_{n-1}}$$

oder

$$Q_n \omega^2 - P_{n-1} = (P_n - Q_{n-1})\omega.$$

Vergleichen wir dies mit

$$C\omega^2 + A = B\omega,$$

so erhellt, da A, B, C ohne gemeinsamen Teiler sind, und ω irrational ist, daß die erste Gleichung aus der zweiten durch Multiplikation mit einer ganzen Funktion $2V$ hervorgeht. Da $n \geqq 1$, ist $Q_n \neq 0$, also auch $V \neq 0$. Wir haben also:

$$Q_n = 2VC, \qquad P_{n-1} = -2VA, \qquad P_n - Q_{n-1} = 2VB.$$

Setzen wir noch $P_n = VB + U$, so haben wir:

$$P_n = VB + U, \quad Q_n = 2VC, \quad P_{n-1} = -2VA, \quad Q_{n-1} = -VB + U.$$

Der Identität

$$P_n Q_{n-1} - Q_n P_{n-1} = (-1)^n$$

entnehmen wir:

$$U^2 - V^2 B^2 + 4 V^2 A C = (-1)^n, \text{ d. h. } U^2 - V^2 D = (-1)^n.$$

Es ist also

$$\varepsilon = U + V\sqrt{D}$$

eine Einheit, und zwar wegen $V \neq 0$ sicher keine triviale. Die Existenz nicht trivialer Einheiten im reellen Körper $K(\sqrt{D})$ ist also erwiesen.

Wir fragen nun nach Einheiten ε, deren Betrag $= 1$ ist. Aus $|\varepsilon| = 1$ und $|N(\varepsilon)| = |\varepsilon\varepsilon'| = 1$ folgt $|\varepsilon'| = 1$. Nun kann, wenn $V \neq 0$ ist, ersichtlich nicht gleichzeitig $|U + V\sqrt{D}| = 1$ und $|U - V\sqrt{D}| = 1$ sein. Denn sonst können sich die höchsten Potenzen nicht wegheben. Es ist also $V = 0$ und demnach ε eine triviale Einheit.

Die nicht trivialen Einheiten haben also stets einen Betrag $\neq 1$. Zwei Einheiten $\varepsilon_1, \varepsilon_2$ von gleichem Betrage $|\varepsilon_1| = |\varepsilon_2|$ sind durch eine Relation $\varepsilon_1 = a\varepsilon_2$ verbunden, wo a eine triviale Einheit ist. In der Tat ist $\frac{\varepsilon_1}{\varepsilon_2}$ auch eine Einheit und $\left|\frac{\varepsilon_1}{\varepsilon_2}\right| = 1$, so daß $\frac{\varepsilon_1}{\varepsilon_2} = a$ ist.

Da mit ε auch $\frac{1}{\varepsilon}$ eine Einheit ist, gibt es sicher Einheiten, deren Betrag > 1 ist. Von diesen seien die Einheiten $a\varepsilon_0$ jene mit dem kleinsten Betrag > 1. Die triviale Einheit a werde so gewählt, daß

$$N(a\varepsilon_0) = a^2 N(\varepsilon_0) = 1 \text{ oder } g$$

wird. Das Vorzeichen von a ist dabei noch beliebig und werde irgendwie fest gewählt. Die so normierte Einheit nennen wir die Grundeinheit des Körpers. Sie werde künftighin mit ε_0 bezeichnet. Es ist also $N(\varepsilon_0) = 1$ oder g.

Mit ε_0 sind auch alle Funktionen $\varepsilon = a \cdot \varepsilon_0^k$ (a eine Einheit, k irgendeine positive oder negative Zahl) Einheiten.

Satz. Jede Einheit von $K(\sqrt{D})$ hat die Form

$$\varepsilon = a \cdot \varepsilon_0^k.$$

Beweis. Wäre ε nicht in dieser Form enthalten, so müßte sich wegen $|\varepsilon_0| > 1$ eine Zahl ν so finden lassen, daß

$$|\varepsilon_0^\nu| < |\varepsilon| < |\varepsilon_0^{\nu+1}|.$$

Gleichheitszeichen könnten nicht stehen, da sich Einheiten gleichen Betrages nur um triviale Einheiten als Faktor unterscheiden, und somit ε doch in die Form $\varepsilon = a\varepsilon_0^k$ zu setzen wäre.

Aus unserer Ungleichung folgt

$$1 < |\varepsilon_0^{-\nu} \cdot \varepsilon| < |\varepsilon_0|.$$

Nun ist aber $\varepsilon_0^{-r}\varepsilon$ auch eine Einheit. Es gäbe also, entgegen der Definition der Grundeinheit, doch eine Einheit, deren Betrag zwischen 1 und $|\varepsilon_0|$ liegt. Widerspruch.

Für die Normen der Einheiten finden wir

$$N(\varepsilon) = a^2 (N(\varepsilon))^k = \begin{cases} a^2, & \text{wenn } N(\varepsilon_0) = 1, \\ a^2 g^k, & \text{wenn } N(\varepsilon_0) = g. \end{cases}$$

Wenn also $N(\varepsilon_0) = 1$ ist, sind die Normen quadratische Reste; für $N(\varepsilon_0) = g$ können sie jede rationale Einheiten sein.

Satz. Ist $K(\sqrt{D})$ ein reeller quadratischer Körper, wo D eine Primfunktion ist, und ist ε_0 seine Grundeinheit, so haben wir

$$N(\varepsilon_0) = g.$$

Beweis. Wäre $N(\varepsilon_0) = 1$, so könnten wir nach dem Hilfssatz des § 11 eine ganze Funktion β des Körpers finden, so daß $\varepsilon_0 = \frac{\beta'}{\beta}$ ist. Dann wäre $\beta' = \varepsilon_0 \beta$, also β und β' assoziiert. Es wäre also $(\beta) = (\beta')$, und somit (β) ein ambiges Hauptideal. Nach § 6 hat also (β) die Gestalt

$$\beta = (A)\mathfrak{p}_1 \mathfrak{p}_2 \cdots \mathfrak{p}_r,$$

wo die $\mathfrak{p}_\nu$ voneinander verschiedene Primideale sind, welche in der Diskriminante aufgehen. Da D Primfunktion ist, gibt es nur ein Primideal dieser Art:

$$\mathfrak{p} = (D, \sqrt{D}) = (\sqrt{D}).$$

A ist rational ganz. Also hat (β) eine der Formen

$$(\beta) = (A) \quad \text{oder} \quad \beta = A(\sqrt{D}).$$

Es ist also

$$\beta = A\varepsilon \quad \text{oder} \quad (\beta) = A\sqrt{D}\,\varepsilon,$$

wo ε eine Einheit ist, somit entweder

$$\varepsilon_0 = \frac{A\varepsilon'}{A\varepsilon} = \frac{\varepsilon'}{\varepsilon} = a \cdot \varepsilon'^2 \quad \text{oder} \quad \varepsilon_0 = \frac{-A\sqrt{D}\,\varepsilon'}{A\sqrt{D}\,\varepsilon} = -a\,\varepsilon'^2,$$

so daß ε_0 nicht die Grundeinheit wäre. Also ist $N(\varepsilon_0) = g$.

Nehmen wir ein Resultat des nächsten Paragraphen zu Hilfe, so gilt der

Satz. Wenn im reellen Körper $K(\sqrt{D})$ die Diskriminante D durch eine Primfunktion ungeraden Grades teilbar ist, gilt $N(\varepsilon_0) = 1$.

Beweis. Aus der Lösbarkeit der Pellschen Gleichung

$$U^2 - V^2 D = g$$

würde, wenn P unser Primteiler ungeraden Grades ist, die Lösbarkeit der Kongruenz

$$U^2 \equiv g \pmod{P}$$

folgen. Unabhängig von diesem Satz werden wir aber in § 15 zeigen, daß sie nicht lösbar ist. Also ist $N(\varepsilon_0) = 1$.

Nun beweisen wir (unabhängig von dem eben abgeleiteten Resultat) den

Satz. Die Klassenzahl des Körpers $K(\sqrt{D})$, wo D eine Primfunktion ist, ist ungerade, es sei denn, daß D einen geraden Grad hat, und der Körper imaginär ist (dann ist sie bekanntlich gerade).

Beweis. Wäre nämlich die Klassenzahl gerade, so müßte es mindestens eine von der Hauptklasse verschiedene ambige Klasse $\mathfrak{K}$ geben (deren Quadrat eben die Hauptklasse ist).

Dann gäbe es also ein Nichthauptideal $\mathfrak{a}$, für welches $\mathfrak{a} \sim \mathfrak{a}'$ ist, also $\frac{\mathfrak{a}'}{\mathfrak{a}} = \alpha$, wo α eine ganze oder gebrochene Funktion ist, deren Norm, wie man sich durch Normenbildung überzeugt, eine triviale Einheit a ist. Dabei ist α bis auf eine Körpereinheit festgelegt.

1. Grad von D ungerade. Wir setzen $\alpha = X + Y\sqrt{D}$. Dann soll $X^2 - Y^2 D = a$ sein, wo a eine triviale Einheit und X, Y rational ist. Da nun $Y^2 D$ auch ungeraden Grad hat, könnten sich, wenn $|Y^2 D| \geqq p$ wäre, die höchsten Potenzen von X^2 und $Y^2 D$ nicht heben. Es ist also $|Y^2 D| \leqq p^{-1}$, und somit $|X| = 1$. Daraus folgt

$$a = \operatorname{sgn}(X^2 - Y^2 D) = (\operatorname{sgn} X)^2 = b^2.$$

a ist also quadratischer Rest. Ersetzt man α durch das gleichwertige $\frac{\alpha}{b} = \alpha_1$, so hat man

$$\frac{\mathfrak{a}'}{\mathfrak{a}} = \alpha_1 \quad \text{mit} \quad N(\alpha_1) = 1.$$

2. Grad von D gerade, Körper reell, also $\operatorname{sgn} D = 1$. Sei ε_0 die Grundeinheit. Dann ist $N(\varepsilon_0) = g$. Wäre $N(\alpha)$ Nichtrest, so könnten wir α durch das gleichwertige $\varepsilon_0 \alpha$ ersetzen, dessen Norm dann ein Rest ist. Wir können also voraussetzen, es sei $N(\alpha) = b^2$. Ersetzen wir α durch das gleichwertige $\alpha_1 = \frac{\alpha}{b}$, so haben wir

$$\frac{\mathfrak{a}'}{\mathfrak{a}} = \alpha_1 \quad \text{mit} \quad N(\alpha_1) = 1.$$

Es gilt also in beiden Fällen

$$\frac{\mathfrak{a}'}{\mathfrak{a}} = \alpha_1 \quad \text{mit} \quad N(\alpha_1) = 1.$$

Dann gibt es ein ganzes β, so daß $\alpha_1 = \frac{\beta}{\beta'}$ ist, also

$$\mathfrak{a}\beta = (\mathfrak{a}\beta)'.$$

Das Ideal $\mathfrak{a}\beta$ wäre also ambig. Da D eine Primfunktion ist, hat also, wie schon einmal ausgeführt wurde, $\mathfrak{a}\beta$ entweder die Form (A) oder

$(A\sqrt{D})$. Es ist also auf jeden Fall $\mathfrak{a}\beta$ ein Hauptideal, also wegen $\mathfrak{a} \sim \mathfrak{a}\beta$ unsere Klasse $\mathfrak{K}$ die Hauptklasse, entgegen unserer Annahme.

Beispiel. Der reelle Körper $K(\sqrt{D})$ $(D = t^2 + a_1 t + a_2)$ hat die Grundeinheit

$$\varepsilon_0 = c\left(t + \frac{1}{2}a_1 + \sqrt{D}\right),$$

wo c passend gewählt ist. Seine Norm ist

$$N(\varepsilon_0) = c^2\left(\frac{1}{4}a_1^2 - a_2\right).$$

Da nun

$$D = \left(t + \frac{1}{2}a_1\right)^2 - \left(\frac{1}{4}a_1^2 - a_2\right)$$

ist, ist also $N(\varepsilon_0) = g$ oder 1, je nachdem ob D Primfunktion ist oder nicht. Wir bestätigen also unsere Sätze.

§ 15.

Das Reziprozitätsgesetz.

Wir wollen nun das von Dedekind ohne ausgeführten Beweis angegebene Reziprozitätsgesetz herleiten.

I. Der Ergänzungssatz.

Sei P eine primäre Primfunktion geraden Grades. Dann hat der reelle Körper $K(\sqrt{D})$ die Grundeinheit ε_0 mit der Norm $N(\varepsilon_0) = g$.

Die Pellsche Gleichung

$$X^2 - PY^2 = g$$

ist also lösbar und demnach erst recht die Kongruenz

$$X^2 \equiv g \pmod{P}.$$

Es ist also $\left[\frac{g}{P}\right] = +1$.

Im Körper $K(\sqrt{g})$ ist also die Primfunktion P zerlegbar in zwei (konjugierte) Primideale. Dieser Körper hat aber die Klassenzahl 1, so daß jedes Ideal ein Hauptideal ist. Demnach besteht eine Zerlegung der Form

$$P = (\alpha)\cdot(\alpha'),$$

wo $\alpha = X + Y\sqrt{g}$ eine ganze Funktion des Körpers $K(\sqrt{g})$ ist. Demnach ist

$$P = c(X^2 - gY^2),$$

wo X, Y ganz rational sind, und c eine triviale Einheit ist. P ist also darstellbar in dieser Form.

Sei nun P primär von ungeradem Grade. Wäre $\left[\frac{g}{P}\right] = +1$, so müßte sich P darstellen lassen in der Form

$$P = c(X^2 - gY^2).$$

Da sich die höchsten Potenzen der rechten Seite nicht heben können, ist der Grad der rechten Seite gerade. P kann sich also nicht durch diese Form darstellen lassen.

Es muß also, wenn P ungeraden Grad hat, $\left[\frac{g}{P}\right] = -1$ sein; die Kongruenz

$$X^2 \equiv g \pmod{P}$$

ist also unlösbar. Dies ist die im vorigen Paragraphen verwendete Behauptung.

Sei nun D_1 irgendeine ganze Funktion, Q einer ihrer Primteiler von ungeradem Grade. Sei D_1 darstellbar in der Form

$$D_1 = c(X^2 - gY^2).$$

Setzen wir $\alpha = X + Y\sqrt{g}$, so hat dies die Zerlegung

$$(D_1) = (\alpha)\cdot(\alpha')$$

zur Folge.

Im Körper $K(\sqrt{g})$ ist nun wegen $\left[\frac{g}{Q}\right] = -1$ der Primteiler Q selbst Primideal und geht demnach in einem der Faktoren rechter Hand auf. Da er ein ambiges Primideal ist, geht er in jedem der konjugierten Ideale (α) und (α') gleich oft auf. In D_1 muß er demnach in gerader Potenz aufgehen. Soll sich also D_1 durch unsere Form darstellen lassen, so darf D_1 Primfunktionen ungeraden Grades nur in gerader Potenz enthalten. Ist dies aber der Fall, so können wir D_1 in die Form setzen

$$D_1 = a P_1 P_2 \dots P_n \cdot A^2,$$

wo a eine Einheit, P_ν Primfunktionen geraden Gerades und A eine ganze rationale Funktion sind.

Sei nun

$$P_\nu = c_\nu (X_\nu + Y_\nu \sqrt{g})(X_\nu - Y_\nu \sqrt{g}).$$

Setzen wir

$$A(X_1 + Y_1\sqrt{g})(X_2 + Y_2\sqrt{g}) \dots (X_n + Y_n\sqrt{g}) = X + Y\sqrt{g}$$

und $c = a c_1 c_2 \dots c_n$, so ist

$$D_1 = c(X^2 - Y^2 g).$$

Eine Funktion D_1 ist also dann und nur dann in unserer Form darstellbar, wenn D_1 Primfaktoren ungeraden Grades nur in gerader Potenz enthält.

Ist D_1 speziell quadratfrei, so haben wir den in § 11 verwendeten Satz über die Darstellbarkeit quadratfreier Funktionen durch unsere Form bewiesen.

Sei P eine beliebige primäre Primfunktion. Da stets $\left[\frac{b^2}{P}\right] = +1$ ist, erhält man den Ergänzungssatz:

$$\left[\frac{a}{P}\right] = \left(\frac{a}{p}\right)^r$$

wo $\left(\frac{a}{p}\right)$ das Legendresche Symbol ist.

II. Das Reziprozitätsgesetz für primäre Primfunktionen P und Q.

1. Wenigstens eine der beiden Primfunktionen hat geraden Grad.

Sei $\left[\frac{P}{Q}\right] = +1$. Wir betrachten den Körper $K(\sqrt{P})$. Da $\operatorname{sgn} P = 1$ ist, ist seine Klassenzahl sicher ungerade: $h = 2k+1$. Q ist wegen $\left[\frac{P}{Q}\right] = +1$ im Körper zerlegbar in zwei konjugierte Primideale: $Q = \mathfrak{q}\,\mathfrak{q}'$. Sei $\mathfrak{K}$ die Klasse, der $\mathfrak{q}$ angehört. Nach dem Fermatschen Satze der Gruppentheorie ist $\mathfrak{K}^h$ die Hauptklasse, also $\mathfrak{q}^{2k+1}$ ein Hauptideal (α), wo $\alpha = X + Y\sqrt{P}$ ganz ist. Somit $\mathfrak{q}'^{2k+1} = (\alpha')$. Dies liefert

$$Q^{2k+1} = (\alpha \cdot \alpha') = (X^2 - Y^2 P),$$

also

$$Q^{2k+1} = c \cdot (X^2 - Y^2 \cdot P),$$

wo c eine triviale Einheit.

a) Grad von P ungerade. Dann ist Q von geradem Grade, also auch Q^{2k+1}. Da nun rechter Hand $Y^2 P$ ungeraden, X^2 aber geraden Grad hat, ist $|X^2| > |Y^2 P|$, und wegen

$$\operatorname{sgn} Q = 1 \quad \text{muß sein} \quad 1 = c\,(\operatorname{sgn} X)^2,$$

also c quadratischer Rest: $c = a^2$. Schreiben wir $\frac{X}{a}$, $\frac{Y}{a}$ an Stelle von X und Y, so wird also

$$Q^{2k+1} = X^2 - Y^2 \cdot P.$$

b) Grad von P gerade. Sei $\varepsilon_0 = U + V\sqrt{P}$ die Grundeinheit von $K(\sqrt{P})$. Dann ist $N(\varepsilon_0) = g$. Setzen wir

$$\varepsilon_0 (X + Y\sqrt{P}) = X_1 + Y_1\sqrt{P},$$

so haben wir

$$Q^{2k+1} = c\,(X^2 - Y^2 P) = \frac{c}{N(\varepsilon_0)}\,(X_1^2 - Y_1^2 P) = \frac{c}{g} \cdot (X_1^2 - Y_1^2 P).$$

Nun ist eine der beiden Zahlen c und $\frac{c}{g}$ sicher Rest. Wir können also annehmen, c sei quadratischer Rest: $c = a^2$. Ersetzen wir wieder X und Y durch $\frac{X}{a}$, $\frac{Y}{a}$, so wird

$$Q^{2k+1} = X^2 - Y^2 P.$$

In beiden Fällen erkennen wir, wenn wir die Gleichungen als Kongruenzen schreiben, daß die Kongruenz

$$X^2 \equiv Q^{2k+1} \pmod{P}$$

lösbar ist. Es ist also $\left[\frac{Q^{2k+1}}{P}\right] = +1$ und nach den Multiplikationsregeln, die bei Dedekind angegeben sind,

$$\left[\frac{Q}{P}\right]^{2k+1} = \left[\frac{Q}{P}\right] = +1.$$

Daraus folgt, daß mit $\left[\frac{P}{Q}\right] = -1$ auch $\left[\frac{Q}{P}\right] = -1$ sein muß, da sonst rückschließend ein Widerspruch entstünde. Es ist also $\left[\frac{P}{Q}\right] = \left[\frac{Q}{P}\right]$, wenn wenigstens eine der Primfunktionen geraden Grad hat.

2. P und Q haben ungeraden Grad.

Wenn hier $\left[\frac{P}{Q}\right] = (-1)^n$ ist ($n = 0$ oder 1), so ist nach dem Ergänzungssatz und den Multiplikationsregeln

$$\left[\frac{g^n P}{Q}\right] = \left[\frac{g}{Q}\right]^n \cdot \left[\frac{P}{Q}\right] = (-1)^n \cdot (-1)^n = +1.$$

Es ist also Q im Körper $K(\sqrt{g^n P})$, dessen Klassenzahl des ungeraden Grades von P wegen sicher ungerade $= 2k+1$ ist, zerlegbar: $Q = \mathfrak{q}\,\mathfrak{q}'$. Wieder ist $\mathfrak{q}^{2k+1}$ ein Hauptideal (α), wo $\alpha = X + Y\sqrt{g^n P}$ eine ganze Funktion von $K(\sqrt{g^n P})$ ist. Man erhält wieder

$$Q^{2k+1} = c\,(X^2 - Y^2 g^n P).$$

Q^{2k+1} hat ungeraden, X^2 geraden Grad. Diesmal rührt also der höchste Koeffizient rechter Hand von $Y^2 g^n P$ her. Wegen

$$\operatorname{sgn} P = \operatorname{sgn} Q = 1 \quad \text{ist also} \quad 1 = -c\,g^n (\operatorname{sgn} Y)^2.$$

c hat also die Form $c = -g^{-n} a^2$.

Ersetzt man wieder X und Y durch $\frac{X}{a}$ und $\frac{Y}{a}$, so wird

$$Q^{2k+1} = -g^{-n}(X^2 - Y^2 g^n P).$$

Dies zeigt also die Lösbarkeit der Kongruenz

$$X^2 \equiv -g^n Q^{2k+1} \pmod{P},$$

so daß

$$\left[\frac{-g^n Q^{2k+1}}{P}\right] = +1, \quad \text{also} \quad \left[\frac{Q}{P}\right]^{2k+1} = \left[\frac{-1}{P}\right] \cdot \left[\frac{g^n}{P}\right].$$

Wir haben also

$$\left[\frac{Q}{P}\right] = \left[\frac{Q}{P}\right]^{2k+1} = \left(\frac{-1}{p}\right) \cdot (-1)^n = \left(\frac{-1}{p}\right) \cdot \left[\frac{P}{Q}\right].$$

Im ganzen ist also

$$\left[\frac{P}{Q}\right]\cdot\left[\frac{Q}{P}\right]=1 \quad \text{oder} \quad \left(\frac{-1}{p}\right),$$

je nachdem wenigstens eine der Primfunktionen geraden Grad hat oder beide ungeraden Grades sind.

Nennen wir also die Grade μ und ν, so ist damit das Reziprozitätsgesetz bewiesen:

$$\left[\frac{P}{Q}\right]\cdot\left[\frac{Q}{P}\right]=\left(\frac{-1}{p}\right)^{\mu\nu}.$$

§ 16.

Verallgemeinerung.

Seien nun M und N zwei beliebige teilerfremde Funktionen, davon N primär. $N=Q_1Q_2\ldots$ sei die Zerlegung von N in Primfunktionen.

Wir führen nun das dem Jacobischen entsprechende Symbol ein:

$$\left[\frac{M}{N}\right]=\prod_i\left[\frac{M}{Q_i}\right].$$

Das Symbol hat folgende Eigenschaften, die unmittelbar aus denen von $\left[\frac{M}{Q}\right]$ folgen:

1. $\left[\frac{M_1}{N}\right]\cdot\left[\frac{M_2}{N}\right]=\left[\frac{M_1M_2}{N}\right]$, weil $\left[\frac{M_1}{Q_i}\right]\cdot\left[\frac{M_2}{Q_i}\right]=\left[\frac{M_1M_2}{Q_i}\right]$.

2. Sei

$$M_1\equiv M_2 \pmod N.$$

Dann ist erst recht

$$M_1\equiv M_2 \pmod{Q_i}, \quad \text{also} \quad \left[\frac{M_1}{Q_i}\right]=\left[\frac{M_2}{Q_i}\right].$$

Es ist also

$$\left[\frac{M_1}{N}\right]=\left[\frac{M_2}{N}\right].$$

3. Es sei auch $M=P_1P_2\ldots$ primär. $\mu_1,\mu_2,\ldots$ seien die Grade von $P_1,P_2,\ldots$, $\nu_1,\nu_2,\ldots$ die von $Q_1,Q_2,\ldots$, μ sei der von M und ν der von N. Dann ist:

$$\mu=\sum_i\mu_i, \quad \nu=\sum_k\nu_k, \quad \text{also} \quad \mu\nu=\sum_{i\,k}\mu_i\nu_k.$$

Wegen

$$\left[\frac{N}{M}\right]=\prod_{i,k}\left[\frac{Q_k}{P_i}\right], \quad \left[\frac{M}{N}\right]=\prod_{i,k}\left[\frac{P_i}{Q_k}\right]$$

gilt

$$\left[\frac{N}{M}\right]\left[\frac{M}{N}\right]=\prod_{i,k}\left(\frac{-1}{p}\right)^{\mu_i\nu_k}=\left(\frac{-1}{p}\right)^{\sum_{i,k}\mu_i\nu_k}=\left(\frac{-1}{p}\right)^{\mu\nu}.$$

Ferner ist

$$\left[\frac{a}{M}\right] = \prod_i \left[\frac{a}{P_i}\right] = \prod_i \left(\frac{a}{p}\right)^{\mu_i} = \left(\frac{a}{p}\right)^{\mu}.$$

Ist also M und N primär und teilerfremd, so gilt das Reziprozitätsgesetz (wenn μ und ν die Grade sind)

$$\left[\frac{M}{N}\right]\left[\frac{N}{M}\right] = \left(\frac{-1}{p}\right)^{\mu\nu}$$

und der Ergänzungssatz

$$\left[\frac{a}{M}\right] = \left(\frac{a}{p}\right)^{\mu}.$$

Die Symbole $\left[\frac{M}{N}\right]$ und $\left[\frac{N}{M}\right]$ sind also dann und nur dann verschieden, wenn gleichzeitig M und N ungeraden Grad haben und $p \equiv 3 \pmod 4$ ist.

Beachten wir

$$\frac{|M|-1}{p-1} = \frac{p^{\mu}-1}{p-1} = 1 + p + p^2 + \ldots + p^{\mu-1} \equiv \mu \pmod 2$$

und analog

$$\frac{|N|-1}{p-1} \equiv \nu \pmod 2,$$

sowie

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = (-1)^{\left(\frac{p-1}{2}\right)^2} \quad \text{und} \quad \left(\frac{a}{p}\right) = a^{\frac{p-1}{2}}$$

(Eulersches Kriterium), so können wir dem Gesetz die Form geben:

$$\left[\frac{M}{N}\right]\left[\frac{N}{M}\right] = (-1)^{\frac{|M|-1}{2}\cdot\frac{|N|-1}{2}}, \qquad \left[\frac{a}{M}\right] = a^{\frac{|M|-1}{2}},$$

in der die Analogie mit dem gewöhnlichen Reziprozitätsgesetze am deutlichsten ist.

Sei nun Δ eine primäre Funktion, die nicht gerade ein volles Quadrat ist. Dann enthält Δ mindestens eine Primfunktion P in ungerader Potenz. Wir setzen $\Delta = P^{2k+1}\Delta_1$, wo Δ_1 prim zu P ist. Nach Dedekind besitzt P mindestens einen Nichtrest B. Wir bestimmen nun die zu Δ prime Funktion F durch die Kongruenzen

$$F \equiv B \pmod P, \qquad F \equiv 1 \pmod{\Delta_1},$$

was immer geht. Dann ist

$$\left[\frac{F}{\Delta}\right] = \left[\frac{F}{P}\right]^{2k+1} \cdot \left[\frac{F}{\Delta_1}\right] = \left[\frac{B}{P}\right]^{2k+1} = -1.$$

Nun betrachten wir die Summe

$$S = \sum_{(G,\Delta)=1} \left[\frac{G}{\Delta}\right],$$

erstreckt über ein Repräsentantensystem der primen Restklassen modulo Δ.

Mit G durchläuft dann auch FG ein solches Repräsentantensystem. Es ist also

$$S = \sum_{(G,\,\Delta)=1} \left[\frac{FG}{\Delta}\right] = \left[\frac{F}{\Delta}\right] \cdot \sum_{(G,\,\Delta)=1} \left[\frac{G}{\Delta}\right] = -S.$$

Daraus folgt

$$S = 0.$$

Wenn also Δ kein volles Quadrat ist, verschwindet $\sum \left[\frac{G}{\Delta}\right]$ erstreckt über ein Repräsentantensystem primer Restklassen.

Es sei nun $K(\sqrt{D})$ irgendein Körper. Dann führen wir die Größen ein:

$$\sigma_\nu = \sum_{|F|=p^\nu} \left[\frac{D}{F}\right],$$

wo die Summe über alle primären, zu D primen Funktionen F vom ν-ten Grad zu erstrecken ist.

Satz. Ist $D \neq g$ und D vom n-ten Grade, so gilt

$$\sigma_\nu = 0 \quad \text{für} \quad \nu \geqq n.$$

Beweis. Wir setzen $D = a\Delta$, wo $a = \operatorname{sgn} D$ ist. Dann ist Δ wegen $D \neq g$ quadratfrei und primär, also sicher kein volles Quadrat.

Nach dem Reziprozitätsgesetze ist nun (ν Grad von F)

$$\left[\frac{D}{F}\right] = \left[\frac{a}{F}\right]\left[\frac{\Delta}{F}\right] = \left(\frac{a}{p}\right)^\nu \cdot \left(\frac{-1}{p}\right)^{\nu n} \cdot \left[\frac{F}{\Delta}\right].$$

Setzen wir also $b = a \cdot (-1)^n$, so wird

$$\left[\frac{D}{F}\right] = \left(\frac{b}{p}\right)^\nu \cdot \left[\frac{F}{\Delta}\right].$$

Sei nun $\nu \geqq n$. Dann hat F die Form $F = K \cdot \Delta + A$, wo $|A| < |\Delta|$ und K ganz, primär und von Null verschieden ist. F durchläuft nun alle primären zu Δ primen Funktionen des Grades ν, wenn A alle zu Δ primen (nicht nur primären) Funktionen niedrigeren Grades als Δ (also ein Repräsentantensystem primer Restklassen) durchläuft, und gleichzeitig unabhängig K alle ganzen primären Funktionen $(\nu - n)$-ten Grades. Für $\nu \geqq n$ ist also

$$\sigma_\nu = \sum_{|F|=p^\nu} \left[\frac{D}{F}\right] = \left(\frac{b}{p}\right)^\nu \cdot \sum_{|K|=p^{\nu-n}} \sum_{\substack{(A,\,\Delta)=1 \\ |A|<\Delta}} \left[\frac{K\Delta + A}{\Delta}\right] = \left(\frac{b}{p}\right)^\nu \cdot \sum_{A} \left[\frac{A}{\Delta}\right] \cdot \sum_{K} 1.$$

Nach dem vorhin Gezeigten gilt also die Behauptung.

(Eingegangen am 14. Oktober 1921.)