[6] I. Kaplansky, *Fröhlich's local quadratic forms*, J. Reine Angew. Math. 239 (1969), pp. 74–77.
[7] T. Y. Lam, *The algebraic theory of quadratic forms*, W. A. Benjamin, Reading, Massachusetts, 1973.
[8] A. Prestel, *Remarks on the Pythagoras and Hasse number of real fields*, preprint.
[9] W. Scharlau, *Quadratic forms*, Queen's papers on pure and applied mathematics No. 22, Kingston, Ontario, 1969.
[10] R. Ware, *Hasse principles and the u-invariant over formally real fields*, Nagoya Math. J. 61 (1976), pp. 117–125.

PENNSYLVANIA STATE UNIVERSITY
University Park, Pennsylvania 16802

Received on 27.7.1978
and in revised form on 9.2.1979 (1091)

ACTA ARITHMETICA
XXXIX (1981)

Komposition und Klassenzahlen binärer quadratischer Formen

von

HORST PFEUFFER (Mainz)

Die klassische Kompositionstheorie quadratischer Formen in zwei Variablen von Gauss ([1], Artikel 234–261, 286–287) und Dedekind ([2], X. Supplement) zur Bestimmung der Anzahl der Geschlechter fester Diskriminante kann mittels der Idealtheorie quadratischer Zahlkörper begründet werden (etwa [4], S. 261–292), wobei sich ein Zusammenhang zwischen Klassenzahlen quadratischer Formen und Ringklassenzahlen des Zahlkörpers ergibt. Eine direkte Übertragung auf andere Grundringe als $\mathbf{Z}$ scheint nur möglich zu sein, wenn man sich auf Ideale beschränkt, die eine Modulbasis haben (vergl. [11] und [12]). Betrachtet man jedoch quadratische Formen auf projektiven Moduln A vom Rang zwei mit endlich vielen, aber nicht notwendig nur zwei Erzeugenden über einem Dedekind-Ring $\mathfrak{o}$, so ergibt sich aus der *Komposition von Moduln*, wenn der Quotientenkörper K von $\mathfrak{o}$ ein algebraischer Zahlkörper ist, ebenfalls eine *Beziehung zwischen verschiedenen Klassenzahlen*, die hier bewiesen werden soll.

Die auf den K-Vektorraum $V = k \underset{\mathfrak{o}}{\otimes} A$ fortgesetzte quadratische Form q kann durch einen Skalarfaktor, der Klassenzahlen nicht ändert, so normiert werden, daß es Elemente e in V mit $q(e) = 1$ gibt. Da $\operatorname{char} k \neq 2$ vorausgesetzt wird, ist damit V bis auf Isometrie durch seine Diskriminante dV bestimmt. V sei keine hyperbolische Ebene, also $\delta \underset{2}{=} -dV$ kein Quadrat in k; dann ist $K = k(\sqrt{\delta})$ eine quadratische Erweiterung, und die Norm $N = N_{K|k}$ definiert auf dem zweidimensionalen k-Vektorraum K eine quadratische Form, welche 1 darstellt. Die zugehörige symmetrische Bilinearform ist

$$(x, y) = N(x+y) - N(x) - N(y) = S(x\bar{y})$$

mit der Spur $S = S_{K|k}$, ihre Diskriminante $dK \underset{2}{=} -\delta$. Man darf also $V = K$ und $q = N$ annehmen.

Der erzeugende Automorphismus $J: x \to \bar{x}$ von K/k ist eine Isometrie von V, und zwar eine Spiegelung. Die Multiplikation mit γ aus K ist genau dann eine Isometrie, wenn $N(\gamma) = 1$ ist. Die spezielle orthogonale Gruppe $\mathrm{SO}(V)$ kann mit dem Normkern $N_1 = \{\gamma \in K \mid N(\gamma) = 1\} = K^{*(1-J)}$ identifiziert werden.

Grundlage der Kompositionstheorie ist das für zwei $\mathfrak{o}$-Moduln A und B auf K durch

$$AB = \Big\{ \sum_{\text{endl.}} xy \mid x \in A, y \in B \Big\}$$

definierte *Modulprodukt*. Sind A und B endlich erzeugbare $\mathfrak{o}$-Moduln, so auch AB. Ist einer der Moduln ein Ring $\mathfrak{o}'$ mit Eins, so ist das Produkt $\mathfrak{o}'A$ der von A erzeugte $\mathfrak{o}'$-Modul.

Für einen Primdivisor $\mathfrak{p}$ von k bezeichne $\mathfrak{o}_\mathfrak{p}$ den diskreten Bewertungsring aller für $\mathfrak{p}$ ganzen Elemente von k und $A_\mathfrak{p} = \mathfrak{o}_\mathfrak{p} A$ die *Lokalisierung von A nach $\mathfrak{p}$ innerhalb K*. Für endlich erzeugbare $\mathfrak{o}$-Moduln ist $A_\mathfrak{p}$ freier $\mathfrak{o}_\mathfrak{p}$-Modul vom Rang zwei und $A = \bigcap_\mathfrak{p} A_\mathfrak{p}$, wo $\mathfrak{p}$ alle Primdivisoren von k durchläuft. Ist $\mathfrak{O}$ der ganze Abschluß von $\mathfrak{o}$ in K, so besteht der ganze Abschluß $\mathfrak{O}_\mathfrak{p} = \mathfrak{o}_\mathfrak{p}\mathfrak{O} = \bigcap_{\mathfrak{P}\mid\mathfrak{p}} \mathfrak{O}_\mathfrak{P}$ von $\mathfrak{o}_\mathfrak{p}$ in K aus den für $\mathfrak{p}$ ganzen Elementen von K und ist ein semilokaler Hauptidealring. $\mathfrak{O}_\mathfrak{p}$ hat eine $\mathfrak{p}$-Ganzheitsbasis $\{1, b\}$.

Die endlich erzeugbaren $\mathfrak{o}$-Moduln $A \subseteq K$ vom Rang zwei sind *Gitter* auf V im Sinne von O'Meara. Zu jedem von ihnen gibt es, da auch $\mathfrak{O}$ endlich erzeugbar ist ([6], § 127), ein Element α von $\mathfrak{o}$ mit $\mathfrak{O}A \subseteq \frac{1}{\alpha} A$ oder $\alpha\mathfrak{O}A \subseteq A$ ([8], 81.1), das heißt das Vielfachenideal $\alpha\mathfrak{O}$ in K des Divisors (α) von k besteht aus *Multiplikatoren* von A. Gilt dasselbe für zwei beliebige ganze Divisoren $\mathfrak{a}$ und $\mathfrak{b}$ von k, so auch für ihren größten gemeinsamen Teiler:

$$(\mathfrak{a}, \mathfrak{b})_K A = (\mathfrak{a}_K + \mathfrak{b}_K)A = \mathfrak{a}_K A + \mathfrak{b}_K A \subseteq A.$$

Dabei ist mit $\mathfrak{a}_K = \mathfrak{a}\mathfrak{O}$ das Vielfachenideal in K des Divisors $\mathfrak{a} \in \mathfrak{D}_k$ bezeichnet; das Vielfachenideal in k wird ebenfalls $\mathfrak{a}$ genannt. Es gibt also einen im Teilbarkeitssinne kleinsten ganzen Divisor $\mathfrak{f}$ von k mit $\mathfrak{f}_K A \subseteq A$. Dieser heißt *Führer* von A. Die Moduln, die den Einsdivisor $\mathfrak{e}$ zum Führer haben, sind offenbar die (gebrochenen) Ideale von K. Unter dem Führer von $A_\mathfrak{p}$ hat man die niedrigste Potenz $\mathfrak{p}^\lambda$ zu verstehen derart, daß alle $\mathfrak{O}_\mathfrak{p}$-Vielfachen von $\mathfrak{p}^\lambda$ Multiplikatoren von $A_\mathfrak{p}$ sind. *Hat A Führer $\mathfrak{f}$, so hat $A_\mathfrak{p}$ Führer $\mathfrak{f}_\mathfrak{p}$*, womit der $\mathfrak{p}$-Anteil von $\mathfrak{f}$ oder auch das Ideal seiner $\mathfrak{o}_\mathfrak{p}$-Vielfachen bezeichnet wird.

Die endlich erzeugbaren Moduln R, die zugleich Ringe mit Eins sind, bestehen aus Elementen von $\mathfrak{O}$. Der Führer von R ist der kleinste Divisor $\mathfrak{f}$ von k mit $\mathfrak{f}_K \subseteq R$. Dann liegt auch der durch $\mathfrak{o}_\mathfrak{f} = \mathfrak{o} + \mathfrak{f}_K$ definierte Ring in R, und durch Lokalisierung nach $\mathfrak{p}$ folgt

$$\mathfrak{o}_\mathfrak{p}\mathfrak{o}_\mathfrak{f} = \mathfrak{o}_\mathfrak{p} \oplus \mathfrak{f}_\mathfrak{p} b \subseteq R_\mathfrak{p} \subseteq \mathfrak{O}_\mathfrak{p} = \mathfrak{o}_\mathfrak{p} \oplus \mathfrak{o}_\mathfrak{p} b,$$

also $R_\mathfrak{p} = \mathfrak{o}_\mathfrak{p} \oplus \mathfrak{p}^\nu b$ mit $\mathfrak{p}^\nu \mid \mathfrak{f}_\mathfrak{p}$. Da $R_\mathfrak{p}$ den Führer $\mathfrak{f}_\mathfrak{p}$ hat, folgt $\mathfrak{p}^\nu = \mathfrak{f}_\mathfrak{p}$, also $R_\mathfrak{p} = \mathfrak{o}_\mathfrak{p}\mathfrak{o}_\mathfrak{f}$ für jedes $\mathfrak{p}$ und damit

$$R = \mathfrak{o}_\mathfrak{f} = \{x \in \mathfrak{O} \mid \text{ex. } \xi \in k\colon\ x \equiv \xi \pmod{\mathfrak{f}}\}.$$

Die *Ordnungen* $\mathfrak{o}_\mathfrak{f}$ sind zwar nicht ganz-abgeschlossen, aber noethersch. Alle ihre Primideale sind maximal, und jedes Ideal hat eine eindeutige Darstellung $A = \bigcap_{i=1}^{r} Q_i = \prod_{i=1}^{r} Q_i$ durch paarweise teilerfremde Primärideale Q_i, die aber nicht Potenzen ihres zugehörigen Primideals P_i zu sein brauchen. Ein Ideal ist genau dann zu A teilerfremd, wenn es zu jedem P_i teilerfremd ist ([6], § 112, 113, 127). *Die Primidealteiler P von $\mathfrak{f}_K$ in $\mathfrak{o}_\mathfrak{f}$ entsprechen eineindeutig den Primdivisoren $\mathfrak{p} \mid \mathfrak{f}$* mittels $\mathfrak{p} = P \cap \mathfrak{o}$, $P = \mathfrak{p} + \mathfrak{f}_K$. Für diese ist $P_\mathfrak{p}$ das einzige maximale Ideal von $\mathfrak{o}_\mathfrak{p}\mathfrak{o}_\mathfrak{f}$, während für $\mathfrak{p} \nmid \mathfrak{f}$ stets $\mathfrak{o}_\mathfrak{p}\mathfrak{o}_\mathfrak{f} = \mathfrak{O}_\mathfrak{p}$ wird. In jedem Falle ist

$$\mathfrak{o}_\mathfrak{p}\mathfrak{o}_\mathfrak{f} = \{x \in \mathfrak{O}_\mathfrak{p} \mid \text{ ex. } \xi \in k\colon\ x \equiv \xi \pmod{\mathfrak{f}_\mathfrak{p}}\}$$

und hat die $\mathfrak{o}_\mathfrak{p}$-Basis $\{1, b_\mathfrak{f}\}$, wo $b_\mathfrak{f} = \pi^\lambda b$ mit $\mathfrak{f}_\mathfrak{p} = \mathfrak{p}^\lambda$ und einem Primelement π für $\mathfrak{p}$ ist.

Für zwei Elemente $x, y \in K$ sei

$$d(x, y) = \det \begin{pmatrix} 2N(x) & S(x\bar{y}) \\ S(\bar{x}y) & 2N(y) \end{pmatrix}.$$

Bekanntlich ist $\mathfrak{d}_{K/k}$ der größte gemeinsame Teiler aller $d(x, y)$ mit $x, y \in \mathfrak{O}$. Der größte gemeinsame Teiler der $d(x, y)$ mit $x, y \in A$ ist das *Diskriminantenideal* $\mathfrak{d}A$ (in [8] volume genannt) des $\mathfrak{o}$-Moduls A, sein $\mathfrak{p}$-Anteil ist $\mathfrak{d}A_\mathfrak{p} = d(x, y)\mathfrak{o}_\mathfrak{p}$ mit einer beliebigen $\mathfrak{o}_\mathfrak{p}$-Basis $\{x, y\}$ von $A_\mathfrak{p}$, insbesondere ist $\mathfrak{d}_\mathfrak{p} = d(1, b)\mathfrak{o}_\mathfrak{p}$ der $\mathfrak{p}$-Anteil von $\mathfrak{d}_{K/k}$. Der $\mathfrak{o}$-Modul $R = \mathfrak{o}_f$ hat Diskriminantenideal

$$\mathfrak{d}R = \mathfrak{f}^2 \mathfrak{d}_{K/k},$$

wie man durch lokale Betrachtung sieht. Die Norm dieses Moduls im Sinne von O'Meara [8] ist der größte gemeinsame Teiler $\mathfrak{n}R = 2\mathfrak{o}$ aller $(x, x) = 2N(x)$ mit $x \in R$. Hier ist es zweckmäßiger, die *Norm eines Moduls A* als den größten gemeinsamen Teiler $N(A) = \frac{1}{2}\mathfrak{n}A$ aller $N(x)$ mit $x \in A$ zu definieren wie Eichler [5].

Ist $a \in K^*$, so hat aA denselben Führer wie A und die Invarianten $\mathfrak{d}(aA) = N(a)^2\mathfrak{d}A$ und $N(aA) = N(a)N(A)$. Die Moduln $a\mathfrak{o}_\mathfrak{f}$ bilden eine

zu $K^*/u_\mathfrak{f}$ isomorphe Gruppe $\mathscr{H} = \mathscr{H}_\mathfrak{f}$, wo $u_\mathfrak{f}$ die Einheitengruppe von $o_\mathfrak{f}$ bezeichnet. Im Falle $\mathfrak{f} = e$ ist dies die Hauptdivisorgruppe $\mathscr{H}_K$ von K. Ebenso bilden die Moduln $ao_\mathfrak{f}$ mit $a \in \mathscr{D}_k$ eine zur Divisorengruppe $\mathscr{D}_k$ von k isomorphe Gruppe. Sie haben den Führer $\mathfrak{f}$, während dies für $a_K \cap o_\mathfrak{f}$ nicht zu gelten braucht.

Satz 1. *Folgende Bedingungen für den o-Modul A auf K sind gleichbedeutend:*

(1) *A hat Multiplikatorenring $o_\mathfrak{f}$.*

(2) *A hat den Führer $\mathfrak{f}$.*

(3) *Es gibt $a \in K$ so, daß aA ein zu $\mathfrak{f}_K$ primes Ideal von $o_\mathfrak{f}$ ist.*

(4) $A\bar{A} = N(A)o_\mathfrak{f}$.

(5) $o_\mathfrak{f} A \subseteq A$ *und es gibt o-Moduln A' mit* $AA' = o_\mathfrak{f}$.

(6) $\mathfrak{d}A = N(A)^2 \mathfrak{f}^2 \mathfrak{d}_{K|k}$.

Beweis. (1⇒2): Wegen $o_\mathfrak{f} = o + \mathfrak{f}_K$ gilt $o_\mathfrak{f} A \subseteq A \Leftrightarrow \mathfrak{f}_K A \subseteq A$.

(2⇒3): Durch einen Faktor aus K^* ist $A \subseteq o_\mathfrak{f}$ erreichbar. Lokal ist dann für $\mathfrak{p} \nmid \mathfrak{f}$

$$\mathfrak{O}_\mathfrak{p} = o_\mathfrak{p} \mathfrak{f}_K \subseteq o_\mathfrak{p}(A + \mathfrak{f}_K) \subseteq o_\mathfrak{p} o_\mathfrak{f} = \mathfrak{O}_\mathfrak{p}.$$

Für Primdivisoren $\mathfrak{p} | \mathfrak{f}$ sei $\pi^\nu x_0 = \pi^\nu(a_0 + \beta_0 b_\mathfrak{f})$ unter den Elementen $x = a + \beta b_\mathfrak{f} \in A_\mathfrak{p}$ mit minimalen Teiler $\mathfrak{p}^\nu = ao_\mathfrak{p} + \beta o_\mathfrak{p}$ gewählt. Damit ist $A_\mathfrak{p} \subseteq \pi^\nu o_\mathfrak{p} o_\mathfrak{f}$. Falls $a_0 \notin \mathfrak{p}$ für $\pi^\nu x_0 \in A_\mathfrak{p}$ vorkommt, ist $A_\mathfrak{p} \nsubseteq \pi^\nu P_\mathfrak{p} = \pi^\nu(\mathfrak{p} \oplus \oplus o_\mathfrak{p} b_\mathfrak{f})$ und man setzt $a_\mathfrak{p} = \pi^{-\nu}$. Falls stets $a_0 \in \mathfrak{p}$, also $\beta_0 \notin \mathfrak{p}$ ist, folgt $x - \beta\beta_0^{-1} x_0 \in A_\mathfrak{p} \cap o_\mathfrak{p} \subseteq \mathfrak{p}^{\nu+1}$ für jedes $x \in A_\mathfrak{p}$, das heißt $A_\mathfrak{p} = (A_\mathfrak{p} \cap o_\mathfrak{p}) \oplus \oplus \mathfrak{p}_\nu x_0$. Wegen $\bar{x}_0 \in \overline{o_\mathfrak{p} o_\mathfrak{f}} = o_\mathfrak{p} o_\mathfrak{f}$ ist $\pi^\nu N(x_0) \in A_\mathfrak{p} \cap o_\mathfrak{p}$. Wegen $S(x_0) = 2a_0 + + \beta_0 \pi^\lambda S(b) \in \mathfrak{p}$ ist $\pi^{-1}\bar{x}_0 \equiv -\pi^{-1} x_0 \pmod{o_\mathfrak{p}}$, also

$$\pi^{-1}\bar{x}_0(A_\mathfrak{p} \cap o_\mathfrak{p}) \subseteq (-\pi^{-1}x_0 + o_\mathfrak{p})(A_\mathfrak{p} \cap o_\mathfrak{p}) \subseteq \pi^{-1}x_0 \mathfrak{p}^{\nu+1} + (A_\mathfrak{p} \cap o_\mathfrak{p}) = A_\mathfrak{p}.$$

Wäre auch $\pi^{\nu-1} N(x_0) \in A_\mathfrak{p} \cap o_\mathfrak{p}$, also $\pi^{-1}\bar{x}_0 \mathfrak{p}^\nu x_0 \subseteq A_\mathfrak{p}$, so folgte daraus $\pi^{-1}\bar{x}_0 A_\mathfrak{p} \subseteq A_\mathfrak{p}$. Da aber wegen $a_0 \in \mathfrak{p}$ und $\beta_0 \notin \mathfrak{p}$ das Basiselement $\pi^{-1} b_\mathfrak{f}$ von $o_\mathfrak{p} o_{\mathfrak{p}^{-1}\mathfrak{f}}$ durch $\pi^{-1} x_0$ ersetzt werden kann, ist

$$o_\mathfrak{p} o_{\mathfrak{p}^{-1}\mathfrak{f}} = o_\mathfrak{p} \oplus o_\mathfrak{p} \pi^{-1} x_0 = o_\mathfrak{p} \oplus o_\mathfrak{p} \pi^{-1} \bar{x}_0,$$

es wäre $o_\mathfrak{p} o_{\mathfrak{p}^{-1}\mathfrak{f}} A_\mathfrak{p} \subseteq A_\mathfrak{p}$ und A hätte nicht den Führer $\mathfrak{f}$. Folglich ist $\pi^{\nu-1} N(x_0) \notin A_\mathfrak{p} \cap o_\mathfrak{p}$ und damit $A_\mathfrak{p} \cap o_\mathfrak{p} = \pi^\nu N(x_0) o_\mathfrak{p}$, also $A_\mathfrak{p} = \pi^\nu x_0 (o_\mathfrak{p} \oplus o_\mathfrak{p} \bar{x}_0) = \pi^\nu x_0 o_\mathfrak{p} o_\mathfrak{f}$. Man setzt $a_\mathfrak{p} = (\pi^\nu x_0)^{-1}$.

Nach dem Approximationssatz gibt es ein $a \in K$ mit

$$a \equiv a_\mathfrak{p} \pmod{a_\mathfrak{p} \mathfrak{f}_\mathfrak{p}} \quad \text{für} \quad \mathfrak{p} | \mathfrak{f},$$
$$a \in \mathfrak{O}_\mathfrak{p} \quad \text{für} \quad \mathfrak{p} \nmid \mathfrak{f}.$$

Damit ist $(aA)_\mathfrak{p} = a_\mathfrak{p} A_\mathfrak{p} \subseteq o_\mathfrak{p} o_\mathfrak{f}$ und $(aA)_\mathfrak{p} \nsubseteq P_\mathfrak{p}$ für $\mathfrak{p} | \mathfrak{f}$ und $(aA)_\mathfrak{p} \subseteq \mathfrak{O}_\mathfrak{p} A_\mathfrak{p} \subseteq A_\mathfrak{p}$ für $\mathfrak{p} \nmid \mathfrak{f}$, das heißt $aA \subseteq o_\mathfrak{f}$ mit $aA \nsubseteq P$ für alle Primidealteiler P von $\mathfrak{f}_K$ in $o_\mathfrak{f}$.

(3⇒4): Da $\overline{aA} = \bar{a}\bar{A}$, $a\bar{a} = N(a)$ und $N(aA) = N(a)N(A)$ ist, kann man annehmen, daß A ein Ideal von $o_\mathfrak{f}$ mit $A + \mathfrak{f}_K = o_\mathfrak{f}$ ist. Wegen $A\bar{A} = \bigcap_\mathfrak{p} (A\bar{A})_\mathfrak{p} = \bigcap_\mathfrak{p} A_\mathfrak{p} \bar{A}_\mathfrak{p}$ und $N(A) o_\mathfrak{f} = \bigcap_\mathfrak{p} N(A) o_\mathfrak{p} o_\mathfrak{f}$ genügt ein lokaler Beweis. Wenn $\mathfrak{p} \nmid \mathfrak{f}$ ist, ist $o_\mathfrak{p} o_\mathfrak{f} = \mathfrak{O}_\mathfrak{p}$ Hauptidealring, etwa $A_\mathfrak{p} = x\mathfrak{O}_\mathfrak{p}$, also $\bar{A}_\mathfrak{p} = \bar{x}\mathfrak{O}_\mathfrak{p}$ und $N(A)_\mathfrak{p} = N(x) o_\mathfrak{p}$, folglich $A_\mathfrak{p} \bar{A}_\mathfrak{p} = x\bar{x}\mathfrak{O}_\mathfrak{p} = N(A) o_\mathfrak{p} o_\mathfrak{f}$. Wenn $\mathfrak{p} | \mathfrak{f}$ ist, liegt $o_\mathfrak{p} \mathfrak{f}_K$ im maximalen Ideal von $o_\mathfrak{p} o_\mathfrak{f}$, $A_\mathfrak{p}$ aber nicht, also $A_\mathfrak{p} = o_\mathfrak{p} o_\mathfrak{f}$ und $A_\mathfrak{p} \bar{A}_\mathfrak{p} = o_\mathfrak{p} o_\mathfrak{f} = N(A) o_\mathfrak{p} o_\mathfrak{f}$, da $A_\mathfrak{p}$ Einheiten von $o_\mathfrak{p} o_\mathfrak{f}$ enthält.

(4⇒5): Der Multiplikatorenring von A ist endlich erzeugbarer o-Modul, etwa $o_\mathfrak{b}$. Da (1⇒4) schon bewiesen ist, folgt $N(A) o_\mathfrak{b} = A\bar{A} = N(A) o_\mathfrak{f}$, also $o_\mathfrak{f} A = o_\mathfrak{b} A \subseteq A$. Mit $A' = N(A)^{-1}\bar{A}$ ist $AA' = o_\mathfrak{f}$.

(5⇒6): Es gibt endlich viele $y_i \in A'$ mit $\sum_i A_\mathfrak{p} y_i = o_\mathfrak{f}$. Da $Ay_i \subseteq o_\mathfrak{f}$ und $o_\mathfrak{f} A \subseteq A$ ist, sind alle Ay_i Ideale von $o_\mathfrak{f}$, $A_\mathfrak{p} y_i$ Ideale von $o_\mathfrak{p} o_\mathfrak{f}$ mit $\sum_i A_\mathfrak{p} y_i = o_\mathfrak{p} o_\mathfrak{f}$. Bei $\mathfrak{p} \nmid \mathfrak{f}$ ist jedes Ideal von $o_\mathfrak{p} o_\mathfrak{f} = \mathfrak{O}_\mathfrak{p}$ Hauptideal, bei $\mathfrak{p} | \mathfrak{f}$ ist $o_\mathfrak{p} o_\mathfrak{f}$ lokal, also $A_\mathfrak{p} y_i = o_\mathfrak{p} o_\mathfrak{f}$ für mindestens ein y_i, also stets $A_\mathfrak{p} = x o_\mathfrak{p} o_\mathfrak{f}$ und $\mathfrak{d} A_\mathfrak{p} = N(x)^2 \mathfrak{f}_\mathfrak{p}^2 \mathfrak{d}_\mathfrak{p} = (N(A)^2 \mathfrak{f}^2 \mathfrak{d}_{K|k})_\mathfrak{p}$ für jedes $\mathfrak{p}$.

(6⇒1): Eine $o_\mathfrak{p}$-Basis $\{x, y\}$ von $A_\mathfrak{p}$ ist k-Basis von K, also gilt

$$b_\mathfrak{f} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} \xi & \eta \\ \zeta & \omega \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} \quad \text{mit} \quad \xi, \eta, \zeta, \omega \in k.$$

Da $\{1, b_\mathfrak{f}\}$ ebenfalls Basis von K ist, folgt $\eta, \zeta \in k^*$ und $z = x/y = (\xi z + \eta)/(\zeta z + \omega)$, also $S(z) = (\xi - \omega)/\zeta$, $N(z) = -\eta/\zeta$ und

$$d(x, y) = N(y)^2 \det \begin{pmatrix} 2N(z) & S(z) \\ S(\bar{z}) & 2 \end{pmatrix} = -\frac{N(y)^2}{\zeta^2} \left(4\eta\zeta + (\xi - \omega)^2\right);$$

andererseits $S(b_\mathfrak{f}) = \xi + \omega$, $N(b_\mathfrak{f}) = \xi\omega - \eta\zeta$ und $d(1, b_\mathfrak{f}) = -4\eta\zeta - -(\xi - \omega)^2$. Folglich ist $N(A_\mathfrak{p})^2 = \frac{N(y)^2}{\zeta^2} o_\mathfrak{p}$, also $N(A_\mathfrak{p}) = \frac{N(y)}{\zeta} o_\mathfrak{p}$ und ebenso $N(A_\mathfrak{p}) = \frac{N(x)}{\eta} o_\mathfrak{p}$. Nach Definition ist $N(A_\mathfrak{p}) = N(x) o_\mathfrak{p} + S(x\bar{y}) o_\mathfrak{p} + + N(y) o_\mathfrak{p}$, folglich $\eta \in u_\mathfrak{p}$, falls $N(A_\mathfrak{p}) = N(x) o_\mathfrak{p}$, $(\xi - \omega) \in u_\mathfrak{p}$, falls $N(A_\mathfrak{p}) = S(x\bar{y}) o_\mathfrak{p}$ und $\zeta \in u_\mathfrak{p}$, falls $N(A_\mathfrak{p}) = N(y) o_\mathfrak{p}$ ist, sowie jedenfalls η, $\xi - \omega$, $\zeta \in o_\mathfrak{p}$. Zusammen mit $0 \equiv N(b_\mathfrak{f}) \equiv \xi\omega \pmod{o_\mathfrak{p}}$ folgt $\xi, \omega \in o_\mathfrak{p}$, also $\xi o_\mathfrak{p} + \eta o_\mathfrak{p} + \zeta o_\mathfrak{p} + \omega o_\mathfrak{p} = o_\mathfrak{p}$, was bedeutet, daß zwar $b_\mathfrak{f}$, aber nicht $\pi^{-1} b_\mathfrak{f} = b_{\mathfrak{p}^{-1}\mathfrak{f}}$ Multiplikator von $A_\mathfrak{p}$ ist.

Aus diesem Satz lassen sich die wohlbekannten Tatsachen folgern, daß der Führer additiv, die Norm multiplikativ ist.

Denn hat etwa A den Führer $\mathfrak{f}$ und B den Führer $\mathfrak{p}$, so ist $\mathfrak{f}_K AB \subseteq AB$ und $\mathfrak{g}_K BA \subseteq BA$, also der Führer von AB ein Teiler von $\mathfrak{h} = (\mathfrak{f}, \mathfrak{g})$.

Wenn $a, b \in K$ nach (3) mit $aA + \mathfrak{f}_K = \mathfrak{o}_\mathfrak{f}$ und $bB + \mathfrak{g}_K = \mathfrak{o}_\mathfrak{g}$ gewählt sind, folgt mit $\mathfrak{h}_K = \mathfrak{f}_K + \mathfrak{g}_K$

$$\mathfrak{o}_\mathfrak{h} = \mathfrak{o} + \mathfrak{h}_K = \mathfrak{o}_\mathfrak{f} + \mathfrak{o}_\mathfrak{g} \subseteq \mathfrak{o}_\mathfrak{f}\mathfrak{o}_\mathfrak{g} = abAB + aA\mathfrak{g}_K + bB\mathfrak{f}_K + \mathfrak{f}_K\mathfrak{g}_K$$

$$\subseteq abAB + \mathfrak{g}_K + \mathfrak{f}_K = abAB + \mathfrak{h}_K \subseteq \mathfrak{o}_\mathfrak{f}\mathfrak{o}_\mathfrak{g} + \mathfrak{h}_K \subseteq \mathfrak{o}_\mathfrak{h},$$

und es besteht Gleichheit. Insbesondere *bilden die Moduln vom Führer* $\mathfrak{f}$ *eine multiplikative Gruppe* $\mathscr{M} = \mathscr{M}_\mathfrak{f}$. Die Norm $N\colon \mathscr{M} \to \mathscr{D}_k$ ist ein Gruppenhomomorphismus. Denn in der obigen Situation gilt

$$N(AB)\mathfrak{o}_\mathfrak{h} = AB\overline{AB} = A\bar{A}B\bar{B} = N(A)\mathfrak{o}_\mathfrak{f}N(B)\mathfrak{o}_\mathfrak{g} = N(A)N(B)\mathfrak{o}_\mathfrak{h},$$

also $N(AB) = N(A)N(B)$.

Zwei Moduln A und B sind *isometrisch*, wenn es $\sigma \in O(V)$ mit $B = A^\sigma$ gibt, das heißt, wenn $B = \gamma A$ oder $B = \gamma\bar{A}$ mit $\gamma \in N_1$ ist. Die Moduln $\gamma\mathfrak{o}_\mathfrak{f}$ mit $\gamma \in N_1$ bilden die *engere Hauptklasse* $\mathscr{N} = \mathscr{N}_\mathfrak{f}$, eine Untergruppe von $\mathscr{M}_\mathfrak{f}$.

Die engere Klasse von $A \in \mathscr{M}_\mathfrak{f}$ ist die Nebenklasse $A\mathscr{N}$. Die Klasse von A enthält außerdem noch die engere Klasse $\bar{A}\mathscr{N}$, die genau dann mit $A\mathscr{N}$ zusammenfällt, wenn $O(A) > \mathrm{SO}(A)$ ist. $\mathrm{SO}(A)$ kann mit $N_1 \cap \mathfrak{u}_\mathfrak{f}$ identifiziet werden.

Zwei Moduln A und B sind *verwandt*, wenn es zu jedem ganzen Divisor $\mathfrak{a} \in \mathscr{D}_k$ ein $\sigma \in \mathrm{SO}(V)$ mit $B_\mathfrak{p} = A_\mathfrak{p}^\sigma$ für alle $\mathfrak{p} \mid \mathfrak{a}$ oder — nach dem schwachen Approximationssatz in K gleichbedeutend — wenn es zu jedem Primdivisor $\mathfrak{p}$ ein $\gamma \in N_1$ mit $B_\mathfrak{p} = \gamma A_\mathfrak{p}$ gibt (siehe auch [8], example 102:4). *Verwandte Moduln haben gleiche Norm und Diskriminante*, also *denselben Führer*. Sind A und C verwandt so auch AB und BC für jeden beliebigen Modul B. Für mit $R = \mathfrak{o}_\mathfrak{f}$ verwandte Moduln A und B ist daher AB und wegen $N(A) = N(R) = \mathfrak{e}$ auch $A^{-1} = \bar{A}$ mit R verwandt. Folglich bilden diese Moduln eine Untergruppe $\mathscr{G} = \mathscr{G}_\mathfrak{f}$ von $\mathscr{M}_\mathfrak{f}$, das *Hauptgeschlecht vom Führer* $\mathfrak{f}$. Das Geschlecht von $A \in \mathscr{M}_\mathfrak{f}$ ist $A\mathscr{G}$; es enthält die Klasse von A, denn bekanntlich ([8], 91:4a) gibt es zu jedem $\mathfrak{p}$ stets $\gamma \in N_1$ mit $\bar{A}_\mathfrak{p} = \gamma A_\mathfrak{p}$, was sich auch unten beiläufig ergeben wird und zeigt, daß in der Definition des Geschlechts auch $\sigma \in O(V)$ zugelassen werden darf.

Die Anzahl $h^+(A)$ *der engeren Klassen im Geschlecht von* A *ist offenbar der Index* $h^+ = (\mathscr{G} : \mathscr{N})$.

Satz 2. *Das Hauptgeschlecht vom Führer* $\mathfrak{f}$ *besteht aus allen Moduln* $B = A^{1-J}$, *wo* A *ein Modul vom Führer* $\mathfrak{f}$ *ist* (vergl. [2], § 155, 158).

Beweis. Für jeden Modul A ist $A^{1-J} = A\bar{A}^{-1} = N(A)^{-1}A^2$. In A kann man zu jedem $\mathfrak{p}$ ein Element x mit $N(x)\mathfrak{o}_\mathfrak{p} = N(A)_\mathfrak{p} = N(A_\mathfrak{p})$ wählen. Damit ist

$$\gamma = x^{1-J} = N(x)^{-1}x^2 \in N(x)^{-1}A_\mathfrak{p}^2 = (A^{1-J})_\mathfrak{p},$$

also $\gamma R_\mathfrak{p} \subseteq (A^{1-J})_\mathfrak{p}$ sowie $\gamma \in N_1$. Außerdem ist $N(A^{1-J}) = N(A)N(\bar{A})^{-1} = \mathfrak{e}$, also, da A^{1-J} den Führer $\mathfrak{f}$ hat, $\mathfrak{d}A^{1-J} = \mathfrak{f}^2\mathfrak{d}_{K/k} = \mathfrak{d}R$, $\mathfrak{d}(A^{1-J})_\mathfrak{p} = \mathfrak{d}R_\mathfrak{p} = \mathfrak{d}(\gamma R_\mathfrak{p})$ und somit $(A^{1-J})_\mathfrak{p} = \gamma R_\mathfrak{p}$, das heißt $A_\mathfrak{p} = \gamma\bar{A}_\mathfrak{p}$ für jedes $\mathfrak{p}$. Die Moduln A^{1-J} liegen also alle im Hauptgeschlecht.

Für jeden Modul $B \in \mathscr{G}$ ist $B = A^{1-J}$ mit geeignetem $A \in \mathscr{M}$ zu zeigen. Für fast alle $\mathfrak{p}$ ist sowieso $B_\mathfrak{p} = R_\mathfrak{p}$; sei $\mathfrak{a}$ das Produkt der übrigen Primdivisoren und $\gamma = a^{1-J} \in N_1$ mit $B_\mathfrak{p} = \gamma R_\mathfrak{p}$ für alle $\mathfrak{p} \mid \mathfrak{a}$. Dann gibt es genau einen $\mathfrak{o}$-Modul A auf K mit

$$A_\mathfrak{p} = \begin{cases} aR_\mathfrak{p} & \text{für} \quad \mathfrak{p} \mid \mathfrak{a}, \\ R_\mathfrak{p} & \text{sonst} \end{cases}$$

([8], 81: 14), denn Lokalisierung und Vervollständigung (in [8] localization) an der Stelle $\mathfrak{p}$ bestimmen sich gegenseitig. Da offenbar

$$(\bar{A}^{-1})_\mathfrak{p} = \begin{cases} \bar{a}^{-1}R_\mathfrak{p} & \text{für} \quad \mathfrak{p} \mid \mathfrak{a}, \\ R_\mathfrak{p} & \text{sonst} \end{cases}$$

ist, folgt

$$(A^{1-J})_\mathfrak{p} = \begin{cases} \gamma R_\mathfrak{p} & \text{für} \quad \mathfrak{p} \mid \mathfrak{a}, \\ R_\mathfrak{p} & \text{sonst} \end{cases}$$

also $(A^{1-J})_\mathfrak{p} = B_\mathfrak{p}$ für alle $\mathfrak{p}$ und $A^{1-J} = B$. Mit einem etwas umständlicheren Argument kann man $B = A^{1-J}$ mit $A = \bar{a}B \cap aR$ beweisen, wenn $B_\mathfrak{p} = \gamma R_\mathfrak{p}$ für alle $\mathfrak{p} \mid \mathfrak{d}B$ mit $\gamma = a^{1-J}$ ist, ohne Vervollständigung zu benutzen.

Der Homomorphismus $1-J\colon \mathscr{M} \to \mathscr{G}$ bildet offenbar $a\mathfrak{o}_\mathfrak{f}$ auf $a^{1-J}\mathfrak{o}_\mathfrak{f} \in \mathscr{N}$, also $\mathscr{H}$ auf $\mathscr{N}$ ab. Der Kern $\mathscr{K} = \mathscr{K}_\mathfrak{f}$ besteht aus allen Moduln A mit $A = \bar{A}$ und der gesuchte Index ist

$$h^+ = (\mathscr{G} : \mathscr{N}) = (\mathscr{M} : \mathscr{H}\mathscr{K}).$$

Zu jedem endlich erzeugten $\mathfrak{o}$-Modul A existiert der *größte gemeinsame Teiler* $\mathfrak{A} \in \mathscr{D}_K$ seiner Elemente. Das Vielfachenideal von $\mathfrak{A}$ ist $\mathfrak{O}A$. Daher ist

$$D\colon \begin{cases} \mathscr{M}_\mathfrak{f} \to \mathscr{D}_K, \\ A \to \mathfrak{A} = \mathrm{GGT}(A) \end{cases}$$

ein Gruppenhomomorphismus, der $a\mathfrak{o}_\mathfrak{f}$ $(a \in K^*)$ auf (a) und $\mathfrak{a}\mathfrak{o}_\mathfrak{f}$ $(\mathfrak{a} \in \mathscr{D}_k)$ auf $\mathfrak{a}$ abbildet sowie mit J vertauschbar ist, also die Norm erhält. *Alle Divisoren kommen als größte gemeinsame Teiler vor*, denn zu $\mathfrak{A} \in \mathscr{D}_K$ gibt es Elemente $a \in K$ so, daß $\mathfrak{B} = a\mathfrak{A}$ ganz und prim zu $\mathfrak{f}$ ist. Für jedes solche a liegt $x \in \mathfrak{B}$ mit $x \equiv 1 \pmod{\mathfrak{f}}$ in $B = \mathfrak{B} \cap \mathfrak{o}_\mathfrak{f}$, also ist $B + \mathfrak{f}_K = \mathfrak{o}_\mathfrak{f}$ und B ein $\mathfrak{o}$-Modul vom Führer $\mathfrak{f}$ mit $\mathfrak{o}_K B \subseteq \mathfrak{B} = \prod_\mathfrak{P} \mathfrak{P}^{a_\mathfrak{P}}$. Für jeden Primdivisor $\mathfrak{P} \mid \mathfrak{B}$ kann man speziell $x \in \mathfrak{B}$ mit $v_\mathfrak{P}(x) = a_\mathfrak{P}$ wählen, was $\mathfrak{P}^{a_\mathfrak{P}} \mid \mathrm{GGT}(B)$ zur Folge hat. Es ist $\mathfrak{B} = \mathrm{GGT}(B)$ und $\mathfrak{A} = \mathrm{GGT}(A)$ mit $A = a^{-1}B = a^{-1}(a\mathfrak{A} \cap \mathfrak{o}_\mathfrak{f})$.

Als *Urbilder des Einsdivisors* erhält man auf diese Weise die sämtlichen $\mathfrak{o}$-Moduln $a^{-1}(a\mathfrak{O} \cap \mathfrak{o}_\mathfrak{f})$ mit zu $\mathfrak{f}$ primen $a \in \mathfrak{O}$. Andere Urbilder von $\mathfrak{e}$ gibt

es nicht. In einem $\mathfrak{o}$-Modul $A \in \mathscr{M}$ mit $\mathrm{GGT}(A) = \mathfrak{e}$ gibt es nämlich zu jedem $\mathfrak{p}$ Elemente $a_\mathfrak{p}$ derart, daß $a_\mathfrak{p}$ und $\bar{a}_\mathfrak{p}$ Einheiten für $\mathfrak{p}$ sind, also $N(a_\mathfrak{p}) \in \mathfrak{u}_\mathfrak{p}$ ist. Wegen $N(a_\mathfrak{p}) \in \bar{a}_\mathfrak{p} A_\mathfrak{p} \subseteq \mathfrak{o}_\mathfrak{p} = \mathfrak{o}_\mathfrak{p} \oplus \mathfrak{o}_\mathfrak{p} b$ folgt

$$\mathfrak{o}_\mathfrak{p} \oplus \mathfrak{f}_\mathfrak{p} b = \mathfrak{o}_\mathfrak{p}\mathfrak{o}_\mathfrak{f} \subseteq \bar{a}_\mathfrak{p} A_\mathfrak{p} = \mathfrak{o}_\mathfrak{p} \oplus \mathfrak{p}^\nu b$$

mit geeigneter Potenz $\mathfrak{p}^\nu$. Da mit $A_\mathfrak{p}$ auch $\bar{a}_\mathfrak{p} A_\mathfrak{p}$ den Führer $\mathfrak{f}_\mathfrak{p}$ hat, folgt $\mathfrak{p}^\nu = \mathfrak{f}_\mathfrak{p}$, also $\bar{a}_\mathfrak{p} A_\mathfrak{p} = \mathfrak{o}_\mathfrak{p}\mathfrak{o}_\mathfrak{f}$. Wählt man nach dem starken Approximationssatz $a \in \mathfrak{O}$ so, daß

$$a \equiv \bar{a}_\mathfrak{p} \pmod{\mathfrak{f}_\mathfrak{p}}$$

für alle $\mathfrak{p} \mid \mathfrak{f}$ gilt, so folgt $(aA)_\mathfrak{p} = aA_\mathfrak{p} = \bar{a}_\mathfrak{p} A_\mathfrak{p} = \mathfrak{o}_\mathfrak{p}\mathfrak{o}_\mathfrak{f}$, also $(aA + \mathfrak{f}_K)_\mathfrak{p} = \mathfrak{o}_\mathfrak{p}\mathfrak{o}_\mathfrak{f}$ für diese $\mathfrak{p}$. Das ist von selbst auch für $\mathfrak{p} \nmid \mathfrak{f}$ wahr, also gilt $aA + \mathfrak{f}_K = \mathfrak{o}_\mathfrak{f}$. Zerlegt man $x \in a\mathfrak{O} \cap \mathfrak{o}_\mathfrak{f}$ in $x = y + z$ mit $y \in aA \subseteq a\mathfrak{O}$ und $z \in \mathfrak{f}_K$, so ist $z \in a\mathfrak{O} \cap \mathfrak{f}_K = a\mathfrak{f}_K = aA\mathfrak{f}_K \subseteq aA\mathfrak{o}_\mathfrak{f} = aA$ und damit $x \in aA \subseteq a\mathfrak{O} \cap \mathfrak{o}_\mathfrak{f}$. Es folgt $a\mathfrak{O} \cap \mathfrak{o}_\mathfrak{f} = aA$.

Für zwei zu $\mathfrak{f}$ prime Zahlen $a, b \in \mathfrak{O}$ ist $C = (a\mathfrak{O} \cap \mathfrak{o}_\mathfrak{f})(b\mathfrak{O} \cap \mathfrak{o}_\mathfrak{f}) \subseteq ab\mathfrak{O} \cap \mathfrak{o}_\mathfrak{f}$ ein $\mathfrak{o}$-Modul vom Führer $\mathfrak{f}$ mit $\mathrm{GGT}(C) = (a)(b) = (ab) = \mathrm{GGT}(ab\mathfrak{O} \cap \mathfrak{o}_\mathfrak{f})$, also $N(C) = N(ab\mathfrak{O} \cap \mathfrak{o}_\mathfrak{f})$. Aus $\mathfrak{d}C = \mathfrak{d}(ab\mathfrak{d} \cap \mathfrak{o}_\mathfrak{f})$ nach Satz 1 folgt ([8], 82: 11/11a) $C = ab\mathfrak{O} \cap \mathfrak{o}_\mathfrak{f}$. Da offenbar für zu $\mathfrak{f}$ prime a

$$a^{-1}(a\mathfrak{O} \cap \mathfrak{o}_\mathfrak{f}) = \mathfrak{o}_\mathfrak{f} \Leftrightarrow a \in \mathfrak{o}_\mathfrak{f}$$

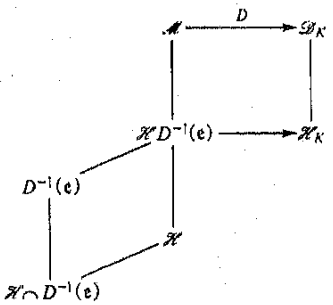
gilt, induziert $a \to a^{-1}(a\mathfrak{O} \cap \mathfrak{o}_\mathfrak{f})$ einen *Gruppenepimorphismus* $(\mathfrak{O}/\mathfrak{f}_K)^* \to D^{-1}(\mathfrak{e})$ *mit Kern* $(\mathfrak{o}_\mathfrak{f}/\mathfrak{f}_K)^*$. Bezeichnet φ_k die Eulersche Funktion des Zahlkörpers k, so ist folglich

$$|D^{-1}(\mathfrak{e})| = \frac{\varphi_K(\mathfrak{f})}{\varphi_k(\mathfrak{f})} = \psi(\mathfrak{f}).$$

Ein Modul $A = w\mathfrak{o}_\mathfrak{f} \in \mathscr{H}$ liegt genau dann in $D^{-1}(\mathfrak{e})$, wenn $(w) = \mathfrak{e}$, also w in der Einheitengruppe $\mathfrak{U}$ von K ist.

$$|\mathscr{H} \cap D^{-1}(\mathfrak{e})| = (\mathfrak{U} : \mathfrak{u}_\mathfrak{f}).$$

Aus



liest man mittels der Isomorphiesätze ab:

$$(1) \qquad (\mathscr{M}_\mathfrak{f} : \mathscr{H}_\mathfrak{f}) = h_K \frac{\psi(\mathfrak{f})}{(\mathfrak{U} : \mathfrak{u}_\mathfrak{f})}$$

mit der *Klassenzahl* h_K *des Körpers* K.

Die Gruppe $\mathscr{K} = \{A \in \mathscr{M} \mid A = \bar{A}\}$ wird von D in die Gruppe $\mathscr{A} = \{\mathfrak{A} \in \mathscr{D}_K \mid \mathfrak{A} = \bar{\mathfrak{A}}\}$ der ambigen Divisoren abgebildet. Wegen $\mathrm{GGT}(a\mathfrak{o}_\mathfrak{f}) = a$ für $a \in \mathscr{D}_k$ ist $\mathscr{D}_k \subseteq D(\mathscr{K}) \subseteq \mathscr{A}$, und $\mathscr{A}$ wird von $\mathscr{D}_k$ und den Verzweigungsprimdivisoren von K erzeugt. Wegen $\mathfrak{P}^2 = \mathfrak{p} \in \mathscr{D}_k$ ist

$$\mathscr{A}/\mathscr{D}_k \cong 3_2^\varkappa$$

mit der Anzahl $\varkappa$ der Primteiler $\mathfrak{p}$ von $\mathfrak{d}_{K/k}$. Kommt in $\mathfrak{A} = D(A)$ mit $A \in \mathscr{K}$ der Verzweigungsprimdivisor $\mathfrak{P}$ mit ungeradem Exponenten $a_\mathfrak{P}$ vor, so kann man $a_\mathfrak{P} = 1$ annehmen. Ein $\mathfrak{o}$-Modul B mit

$$B_\mathfrak{q} = \begin{cases} A_\mathfrak{p}, & \mathfrak{q} = \mathfrak{p}, \\ R_\mathfrak{q}, & \mathfrak{q} \neq \mathfrak{p} \end{cases}$$

([8], 81: 14) hat Führer $\mathfrak{f}$ und $B = \bar{B}$. Für $\mathfrak{B} = \mathrm{GGT}(B)$ gilt

$$\mathfrak{B}_\mathfrak{q} = \begin{cases} \mathfrak{O}_\mathfrak{p} A_\mathfrak{p} = \mathfrak{A}_\mathfrak{p} = \mathfrak{P}, & \mathfrak{q} = \mathfrak{p}, \\ \mathfrak{O}_\mathfrak{q} = \mathfrak{q}^0, & \mathfrak{q} \neq \mathfrak{p} \end{cases}$$

also $\mathfrak{P} = \mathfrak{B} \in D(\mathscr{K})$ und

$$\mathscr{A}/D(\mathscr{K}) \cong 3_2^{\varkappa - \varkappa_\mathfrak{f}}$$

wo $\varkappa_\mathfrak{f}$ *die Anzahl der Verzweigungsprimdivisoren* $\mathfrak{P} \in D(\mathscr{K})$ *ist.* Zu diesen gehören sicher die $\mathfrak{P}$ mit $\mathfrak{P}^2 = \mathfrak{p} \nmid \mathfrak{f}$, denn für solche $\mathfrak{P}$ liegt das oben konstruierte Urbild $P = \mathfrak{P} \cap \mathfrak{o}_\mathfrak{f} \in \mathscr{M}$ in $\mathscr{K}$.

Wenn $\mathfrak{P}^2 = \mathfrak{p} \mid \mathfrak{f}$ ist, erhält man ein Urbild $P \in \mathscr{M}$ durch

$$P_\mathfrak{q} = \begin{cases} b\mathfrak{o}_\mathfrak{p}\mathfrak{o}_\mathfrak{f}, & \mathfrak{q} = \mathfrak{p}, \\ R_\mathfrak{q}, & \mathfrak{q} \neq \mathfrak{p} \end{cases}$$

mit einem beliebigen Primelement b für $\mathfrak{P}$. $P \in \mathscr{K}$ bedeutet $P_\mathfrak{p} = \bar{P}_\mathfrak{p}$; die Existenz von $A \in \mathscr{K}$ mit $\mathrm{GGT}(A) = \mathfrak{P}$ bedeutet die Existenz eines zu $\mathfrak{f}$ primen $a \in \mathfrak{O}$ mit

$$\bar{a}(a\mathfrak{O} \cap \mathfrak{o}^\mathfrak{p}) P_\mathfrak{p} = a(\bar{a}\mathfrak{O} \cap \mathfrak{o}_\mathfrak{f}) \bar{P}_\mathfrak{p}.$$

Mit a ist $N(a)$ zu $\mathfrak{p}$ prim, also

$$\bar{a}(a\mathfrak{O} \cap \mathfrak{o}_\mathfrak{f})_\mathfrak{p} = \mathfrak{O}_\mathfrak{p} \cap \bar{a}\mathfrak{o}_\mathfrak{p}\mathfrak{o}_\mathfrak{f} = \bar{a}\mathfrak{o}_\mathfrak{p}\mathfrak{o}_\mathfrak{f}$$

und die Bedingung gleichbedeutend zu Existenz von $a \in \mathfrak{O}_\mathfrak{p} \setminus \mathfrak{P}$ mit $\bar{a}b\mathfrak{o}_\mathfrak{p}\mathfrak{o}_\mathfrak{f} = a\bar{b}\mathfrak{o}_\mathfrak{p}\mathfrak{o}_\mathfrak{f}$ oder

$$\bar{a}b \in a\bar{b}\mathfrak{o}_\mathfrak{p}\mathfrak{o}_\mathfrak{f},$$

da die umgekehrte Inklusion durch Anwendung von J folgt.

Für eine p-Ganzheitsbasis $\{1, b\}$ ist $b^2 = -n + sb$ mit $n = N(b)$, $s = S(b) \in \mathfrak{o}_\mathfrak{p}$, $\mathfrak{m}_\mathfrak{p} = 2\mathfrak{o}_\mathfrak{p} + s\mathfrak{o}_\mathfrak{p}$ mit der reduzierten Differente $\mathfrak{m} = \partial_{K/k} = S(\mathfrak{D})$ (vergl. [7], S. 420) und $\mathfrak{d}_\mathfrak{p} = (4n - s^2)\mathfrak{o}_\mathfrak{p}$, also $\mathfrak{m}|2$ und $\mathfrak{m}^2|\mathfrak{d}_{K/k}$. Indem man notfalls b durch $b+1$ ersetzt, erreicht man $\mathfrak{m}_\mathfrak{p} = s\mathfrak{o}_\mathfrak{p} \ni 2$. Bei verzweigtem $\mathfrak{p} = \mathfrak{P}^2$ kann man andererseits b als Primelement für $\mathfrak{P}$ wählen und dann $s \in \mathfrak{p}$, n als Primelement für $\mathfrak{p}$ annehmen.

Setzt man in der letztgenannten Normierung $\alpha = a + \beta_1 b$ mit $a, \beta_1 \in \mathfrak{o}_\mathfrak{p}$ an, so muß $a \in \mathfrak{u}_\mathfrak{p}$ sein, und mit $\beta = a^{-1}\beta_1 \in \mathfrak{o}_\mathfrak{p}$ wird

$$\frac{\bar{\alpha} b}{\alpha \bar{b}} = \frac{(n\beta + b)^2}{nN(\alpha)} = \frac{1}{N(\alpha)}\left(n\beta^2 - 1 + \frac{2n\beta + s}{n}\, b\right)$$

genau dann, wenn $2n\beta + s \in n\mathfrak{f}_\mathfrak{p}$, also die Kongruenz

$$\frac{s}{n} \equiv -2\beta \pmod{\mathfrak{f}_\mathfrak{p}}$$

durch $\beta \in \mathfrak{o}_\mathfrak{p}$ lösbar, das heißt $s/n \in \mathfrak{f}_\mathfrak{p} + 2\mathfrak{o}_\mathfrak{p}$ ist.

Wegen $n\mathfrak{o}_\mathfrak{p} = \mathfrak{p}$ ist für $\mathfrak{P}^2 = \mathfrak{p}|\mathfrak{f}$ also

$$\mathfrak{P} \in D(\mathscr{K}) \Leftrightarrow s \in (\mathfrak{f}_\mathfrak{p} + 2\mathfrak{o}_\mathfrak{p})\mathfrak{p}.$$

Um dies mit Hilfe der Invarianten von K/k zu formulieren, braucht man nur $\mathfrak{d}_\mathfrak{p} = d(1, b)\mathfrak{o}_\mathfrak{p} = (4n - s^2)\mathfrak{o}_\mathfrak{p}$ zu beachten. Im Falle $s \in 2\mathfrak{p}$ ist die Bedingung erfüllt, wie immer $\mathfrak{f}_\mathfrak{p}$ aussieht, und $\mathfrak{d}_\mathfrak{p} = 4\mathfrak{p}$. Im Falle $s \notin 2\mathfrak{p}$ bedeutet die Bedingung $s \in \mathfrak{p}\mathfrak{f}_\mathfrak{p}$ und es ist $\mathfrak{d}_\mathfrak{p} = s^2\mathfrak{o}_\mathfrak{p}$. Daher ist

$$\varkappa_\mathfrak{f} = |\{\mathfrak{p} |\ \mathfrak{d}_\mathfrak{p} \subset \mathfrak{f}_\mathfrak{f}^2 \text{ oder } \mathfrak{d}_\mathfrak{p} = 4\mathfrak{p}\}|. \tag{2.1}$$

Die in $\mathscr{K}$ liegenden Moduln $\alpha^{-1}(a\mathfrak{D} \cap \mathfrak{o}_\mathfrak{f})$ mit zu $\mathfrak{f}$ primen $a \in \mathfrak{D}$ sind analog durch

$$\bar{\alpha} \in a\mathfrak{o}_\mathfrak{p}\mathfrak{o}_\mathfrak{f} \quad \text{für alle } \mathfrak{p}|\mathfrak{f}$$

gekennzeichnet, wegen $N(\alpha) \in \mathfrak{u}_\mathfrak{p}$ also durch

$$a^2 \in \mathfrak{o}_\mathfrak{p}\mathfrak{o}_\mathfrak{f} \quad \text{für alle } \mathfrak{p}|\mathfrak{f}.$$

Für $\mathfrak{p} \nmid \mathfrak{f}$ ist dies stets erfüllt.

Das Urbild von $\mathscr{K} \cap D^{-1}(\mathfrak{e})$ bei dem obigen Homomorphismus von $(\mathfrak{D}/\mathfrak{f}_K)^*$ auf $D^{-1}(\mathfrak{e})$ ist die Gruppe

$$\mathfrak{K} = \{a + \mathfrak{f}_K |\ (a + \mathfrak{f}_K)^2 \in (\mathfrak{o}_\mathfrak{f}/\mathfrak{f}_K)^*\},$$

also

$$\mathscr{K} \cap D^{-1}(\mathfrak{e}) \cong \mathfrak{K}/(\mathfrak{o}_\mathfrak{f}/\mathfrak{f}_K).$$

Bei der kanonischen Zerlegung $(\mathfrak{D}/\mathfrak{f}_K)^* \cong \bigtimes_{\mathfrak{p}|\mathfrak{f}} (\mathfrak{D}_\mathfrak{p}/\mathfrak{f}_\mathfrak{p})^*$ zerlegen sich $\mathfrak{K} \cong \bigtimes_{\mathfrak{p}|\mathfrak{f}} \mathfrak{K}_\mathfrak{p}$ mit

$$\mathfrak{K}_\mathfrak{p} = \{a + \mathfrak{f}_\mathfrak{p} |\ (a + \mathfrak{f}_\mathfrak{p})^2 \in (\mathfrak{o}_\mathfrak{p}/\mathfrak{f}_\mathfrak{p})^*\}$$

und $(\mathfrak{o}_\mathfrak{f}/\mathfrak{f}_K)^* \cong \bigtimes_{\mathfrak{p}|\mathfrak{f}} (\mathfrak{o}_\mathfrak{p}/\mathfrak{f}_\mathfrak{p})^*$ entsprechend, also

$$(\mathfrak{K} : (\mathfrak{o}_\mathfrak{f}/\mathfrak{f}_K)^*) = \prod_{\mathfrak{p}|\mathfrak{f}} (\mathfrak{K}_\mathfrak{p} : (\mathfrak{o}_\mathfrak{p}/\mathfrak{f}_\mathfrak{p})^*).$$

Zur Berechnung der Faktoren sei weiterhin $\mathfrak{f}_\mathfrak{p} = \mathfrak{p}^\lambda$, $\{1, b\}$ eine p-Ganzheitsbasis, s und n wie oben und $\mathfrak{p}^\mu = \mathfrak{m}_\mathfrak{p} = 2\mathfrak{o}_\mathfrak{p} + s\mathfrak{o}_\mathfrak{p}$.

Mit dem Ansatz $\alpha \equiv a + \beta b \pmod{\mathfrak{p}^\lambda}$ mit $a, \beta \in \mathfrak{o}_\mathfrak{p}$ hat man $N(\alpha) \equiv a^2 + sa\beta + n\beta^2$ und $\alpha^2 \equiv (a^2 - n\beta^2) + (2a\beta + s\beta^2)b$, also $\alpha + \mathfrak{p}^\lambda \in \mathfrak{K}_\mathfrak{p}$ genau dann, wenn

$$(*) \qquad \begin{aligned} &a^2 + sa\beta + n\beta^2 \notin \mathfrak{p}, \\ &(2a + s\beta)\beta \in \mathfrak{p}^\lambda. \end{aligned}$$

Nach der Größe von λ sind *vier Fälle* zu unterscheiden.

1. Fall: $\lambda \leqslant \mu$ (kommt wegen $\mathfrak{m}|2$ nur bei verzweigtem, geradem $\mathfrak{p}$ vor). Es darf s, $n \in \mathfrak{p}$ angenommen werden. Dann muß $\alpha \in \mathfrak{u}_\mathfrak{p}$ sein und $(2a + s\beta)\beta \in \mathfrak{m}_\mathfrak{p}\beta \subseteq \mathfrak{p}^\mu\mathfrak{o}_\mathfrak{p} \subseteq \mathfrak{p}^\lambda$ gilt stets. Folglich

$$|\mathfrak{K}_\mathfrak{p}| = \varphi(\mathfrak{p}^\lambda)\mathfrak{N}\mathfrak{p}^\lambda.$$

2. Fall: $\mu < \lambda \leqslant 2e - \mu$ mit $e = v_\mathfrak{p}(2)$ (kommt wegen $\mu \geqslant 0$ nur bei geradem $\mathfrak{p}$ mit $\mu < e$ vor). Es ist $v_\mathfrak{p}(s) = \mu$ und aus $(2a + s\beta)\beta \equiv s\beta^2 \equiv 0 \pmod{\mathfrak{p}^{\mu+1}}$ folgt $\beta \in \mathfrak{p}$. Dann muß $\alpha \in \mathfrak{u}_\mathfrak{p}$ sein. Für jedes solche α und $s\beta^2 \notin \mathfrak{p}^\lambda$ ist $(2a + s\beta)\beta \notin \mathfrak{p}^\lambda$, denn sonst wäre $2a\beta \notin \mathfrak{p}^\lambda$, $\lambda > e$ und $\beta \notin \mathfrak{p}^{\lambda - e}$, also wegen $\lambda - e \leqslant e - \mu$ auch $\beta \notin \mathfrak{p}^{e-\mu}$, $s\beta \notin \mathfrak{p}^e = 2\mathfrak{o}_\mathfrak{p}$ und schließlich $(2a + s\beta)\beta\mathfrak{o}_\mathfrak{p} = s\beta^2\mathfrak{o}_\mathfrak{p} \nsubseteq \mathfrak{p}^\lambda$. Es kommt also nur $s\beta^2 \in \mathfrak{p}^\lambda$, das heißt $\beta \in \mathfrak{p}^{\left[\frac{\lambda-\mu+1}{2}\right]}$ in Frage und für diese β folgt, daß

$$(2a + s\beta)\beta \in \mathfrak{p}^{e + \left[\frac{\lambda-\mu+1}{2}\right]} + \mathfrak{p}^{\mu+2\left[\frac{\lambda-\mu+1}{2}\right]} \subseteq \mathfrak{p}^\lambda$$

ist.

Folglich

$$|\mathfrak{K}_\mathfrak{p}| = \varphi(\mathfrak{p}^\lambda)\mathfrak{N}\mathfrak{p}^{\left[\frac{\lambda+\mu}{2}\right]}.$$

3. Fall: $2e - \mu < \lambda$ und $\mathfrak{m}_\mathfrak{p}^2 = \mathfrak{d}_\mathfrak{p}$. Es darf $2 \in s\mathfrak{o}_\mathfrak{p} = \mathfrak{m}_\mathfrak{p}$ angenommen werden. Bei $s\beta \notin 2\mathfrak{o}_\mathfrak{p}$ ist $(2a + s\beta)\beta \notin \mathfrak{p}^\lambda$, denn sonst wäre $s\beta^2\mathfrak{o}_\mathfrak{p} = (2a + s\beta)\beta\mathfrak{o}_\mathfrak{p} \subseteq \mathfrak{p}^\lambda$, $\beta \in \mathfrak{p}^{\left[\frac{\lambda-\mu+1}{2}\right]}$, also doch $s\beta = \mathfrak{p}^{\left[\frac{\lambda+\mu+1}{2}\right]} \subseteq 2\mathfrak{o}_\mathfrak{p}$. Bei $s\beta \in 2\mathfrak{o}_\mathfrak{p}$ ist $\beta = \frac{2}{s}\beta_0$ mit $\beta_0 \in \mathfrak{o}_\mathfrak{p}$ und $(*)$ gleichbedeutend zu

$$(a + \beta_0)^2 + \frac{4n - s^2}{s^2}\beta_0^2 = a^2 + 2a\beta_0 + \frac{4n}{s^2}\beta_0^2 \notin \mathfrak{p},$$

$$(a + \beta_0)\beta_0 \in \mathfrak{p}^{\lambda - 2e + \mu}.$$

Es ist daher notwendig $\alpha+\beta_0 \in \mathfrak{u}_\mathfrak{p}$ und $\beta_0 \in \mathfrak{p}^{\lambda-2e+\mu}$ oder $\beta_0 \in \mathfrak{u}_\mathfrak{p}$ und $\beta_0 \equiv -\alpha \pmod{\mathfrak{p}^{\lambda-2e+\mu}}$, also jedenfalls $\alpha \in \mathfrak{u}_\mathfrak{p}$. Ist umgekehrt $\alpha \in \mathfrak{u}_\mathfrak{p}$ und $\beta_0 \equiv 0,\ -\alpha \pmod{\mathfrak{p}^{\lambda-2e+\mu}}$, so ist entweder $\alpha+\beta_0$ oder β_0 Einheit und stets $(\alpha+\beta_0)\beta_0 \in \mathfrak{p}^{\lambda-2e+\mu}$. Da $\frac{4n-s^2}{s^2}\mathfrak{o}_\mathfrak{p} = \frac{\mathfrak{d}_\mathfrak{p}}{\mathfrak{m}_\mathfrak{p}^2} = \mathfrak{o}_\mathfrak{p}$ angenommen wird, ist auch die erste Bedingung erfüllt. Ein $\beta_0 \bmod \mathfrak{p}^{\lambda-2e+\mu}$ bestimmt $\mathfrak{N}\mathfrak{p}^e$ $\beta \bmod \mathfrak{p}^\lambda$; folglich

$$|\mathfrak{K}_\mathfrak{p}| = 2\varphi(\mathfrak{p}^\lambda)\mathfrak{N}\mathfrak{p}^e.$$

4. Fall: $2e-\mu < \lambda$ und $\mathfrak{p}\mathfrak{m}_\mathfrak{p}^2 \supseteq \mathfrak{d}_\mathfrak{p}$ (kommt nur bei verzweigtem $\mathfrak{p}$ vor). Es darf $s, n \in \mathfrak{p}$ angenommen werden. Aus $4n-s^2 \in \mathfrak{p}\mathfrak{m}_\mathfrak{p}^2 = \mathfrak{p}(4\mathfrak{o}_\mathfrak{p}+s^2\mathfrak{o}_\mathfrak{p})$ folgt dann $s^2 \in \mathfrak{p}(4\mathfrak{o}_\mathfrak{p}+s^2\mathfrak{o}_\mathfrak{p})$, also $s^2 \in 4\mathfrak{p}$ und $s \in 2\mathfrak{p}$. Dann muß $\alpha \in \mathfrak{u}_\mathfrak{p}$ sein und für jedes solche α ist $2\beta\mathfrak{o}_\mathfrak{p} = (2\alpha+s\beta)\beta\mathfrak{o}_\mathfrak{p} \subseteq \mathfrak{p}^\lambda$ genau für $\beta \in \mathfrak{p}^{\lambda-e}$, folglich

$$|\mathfrak{K}_\mathfrak{p}| = \varphi(\mathfrak{p}^\lambda)\mathfrak{N}\mathfrak{p}^e.$$

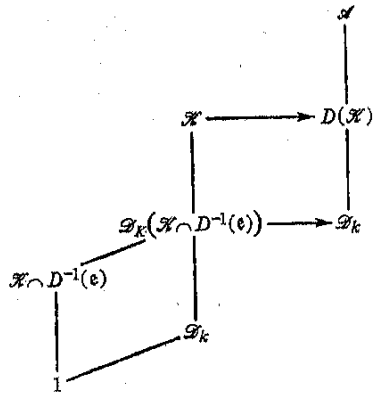
Setzt man für eine Potenz $\mathfrak{p}^\lambda$

$$k(\mathfrak{p}^\lambda) = \begin{cases} \mathfrak{N}\mathfrak{p}^\lambda, & \mathfrak{m}_\mathfrak{p} \subseteq \mathfrak{p}^\lambda, \\ \mathfrak{N}\mathfrak{p}^{\left[\frac{\lambda+\mu}{2}\right]}, & \frac{4}{\mathfrak{m}_\mathfrak{p}} \subseteq \mathfrak{p}^\lambda \subset \mathfrak{m}_\mathfrak{p}, \\ 2\mathfrak{N}\mathfrak{p}^e, & \mathfrak{p}^\lambda \subset \frac{4}{\mathfrak{m}_\mathfrak{p}},\ \mathfrak{d}_\mathfrak{p} = \mathfrak{m}_\mathfrak{p}^2, \\ \mathfrak{N}\mathfrak{p}^e, & \mathfrak{p}^\lambda \subset \frac{4}{\mathfrak{m}_\mathfrak{p}},\ \mathfrak{d}_\mathfrak{p} \subset \mathfrak{m}_\mathfrak{p}^2, \end{cases} \tag{2.2}$$

so ergibt sich zusammen

$$|\mathfrak{K}_\mathfrak{p}| = \varphi(\mathfrak{f}_\mathfrak{p})k(\mathfrak{f}_\mathfrak{p}),$$

und man liest aus



mittels der Isomorphiesätze

$$(\mathscr{K}_\mathfrak{f} : \mathscr{D}_k) = 2^{\varkappa_\mathfrak{f}} \prod_{\mathfrak{p}|\mathfrak{f}} k(\mathfrak{f}_\mathfrak{p}) \tag{2}$$

ab. Nur die Primteiler von $\mathfrak{f}^2\mathfrak{d}_{K/k}$ können zu diesem Produkt beitragen.

Um (1) und (2) zu verbinden, braucht man $\mathscr{H}\cap\mathscr{K}$. $A = x\mathfrak{o}_\mathfrak{f}$ liegt genau dann auch in $\mathscr{K}$, wenn $A^{1-J} = x^{1-J}\mathfrak{o}_\mathfrak{f} = \mathfrak{o}_\mathfrak{f}$, also $x^{1-J} \in \mathfrak{u}_\mathfrak{f}\cap N_1 = W_\mathfrak{f}$ ist. Die Zahlgruppe $U = \{x \in K^* \mid x^{1-J} \in W_\mathfrak{f}\}$ enthält den Kerne k^* und $\mathfrak{u}_\mathfrak{f}$ von $1-J$ und der Abbildung $x \to x\mathfrak{o}_\mathfrak{f}$ von K^* auf $\mathscr{H}$. Durch Anwendung dieser beiden Homomorphismen folgt

$$W_\mathfrak{f}/\mathfrak{u}_\mathfrak{f}^{1-J} \cong U/\mathfrak{u}_\mathfrak{f}k^* \cong \mathscr{H}\cap\mathscr{K}/\mathscr{H}_k.$$

Die Kerne von $1-J$ und der Norm bei Anwendung auf $\mathfrak{u}_\mathfrak{f}$ sind $\mathfrak{u}$ und $W_\mathfrak{f}$. Für $u \in W_\mathfrak{f}$ ist $u^{1-J} = u^2$, also folgt ebenso

$$\mathfrak{u}_\mathfrak{f}^{1-J}/W_\mathfrak{f}^2 \cong \mathfrak{u}_\mathfrak{f}/\mathfrak{u}W_\mathfrak{f} \cong N(\mathfrak{u}_\mathfrak{f})/\mathfrak{u}^2.$$

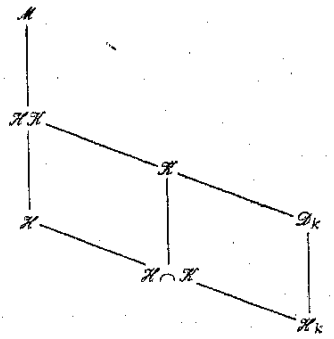
Wenn k *totalreell* und die quadratische Form q *totalpositiv* ist, wird $\delta = -dV$ totalnegativ, also $K = k(\sqrt{\delta})$ *totalimaginär* und bei jeder Einbettung von K in $\boldsymbol{C}$ geht J in das komplexe Konjugieren, $N(u)$ in $|u|_\mathfrak{P}^2$ für die zugehörige unendliche Primstelle $\mathfrak{P}$ über. Aus $u \in W_\mathfrak{f} \subseteq \mathfrak{U}\cap N_1$ folgt also $|u|_\mathfrak{P} = 1$ für alle (endlichen und unendlichen) Primstellen $\mathfrak{P}$ von K, das heißt $W_\mathfrak{f}$ besteht nur aus *Einheitswurzeln* und ist damit endlich und zyklisch. Es ist $(W_\mathfrak{f} : W_\mathfrak{f}^2) = 2$ und

$$Q_\mathfrak{f} = (\mathfrak{u}_\mathfrak{f} : \mathfrak{u}W_\mathfrak{f}) = \big(N(\mathfrak{u}_\mathfrak{f}) : \mathfrak{u}^2\big)$$

kann als *Einheitenindex* von $\mathfrak{o}_\mathfrak{f}$ bezeichnet werden (vergl. [7], S. 536). Man hat $Q_\mathfrak{f} \leqslant Q \leqslant 2$ und

$$(\mathscr{H}_\mathfrak{f}\cap\mathscr{K}_\mathfrak{f} : \mathscr{H}_k) = 2/Q_\mathfrak{f}.$$

In dem Diagramm



sind nunmehr alle Indizes bekannt bis auf den gesuchten, und dieser ergibt sich mittels der Isomorphiesätze aus (1), (2) und (3).

SATZ 3. *Die engere Klassenzahl einer totalpositiven binären quadratischen Form über dem totalreellen algebraischen Zahlkörper k auf dem $\mathfrak{o}$-Modul A mit $\mathfrak{d}A = N(A)^2\mathfrak{f}^2\mathfrak{d}_{K/k}$ ist*

$$h^+ = \frac{\psi(\mathfrak{f})}{\prod\limits_{\mathfrak{p}|\mathfrak{f}} k(\mathfrak{f}_\mathfrak{p})(\mathfrak{U}:\mathfrak{u}_\mathfrak{f})}\,\frac{2}{Q_\mathfrak{f}}\,\frac{h_K}{2^{\varkappa_\mathfrak{f}}h_k}$$

mit den in (2.1) *und* (2.2) *definierten natürlichen Zahlen $\varkappa_\mathfrak{f}$ und $k(\mathfrak{f}_\mathfrak{p})$.*

Der dritte Faktor in diesem Produkt braucht nicht ganz zu sein. Er hat höchstens den Nenner $2/Q_\mathfrak{f}$. Der erste Faktor ist vermutlich ganz; jedenfalls hat er höchstens den Teiler

$$k_\mathfrak{f} = \left(\mathscr{H}_k\left(\mathscr{H}\cap\mathscr{K}\cap D^{-1}(\mathfrak{e})\right):\mathscr{H}_k\right) = |\mathscr{H}\cap\mathscr{K}\cap D^{-1}(\mathfrak{e})| = (\mathfrak{U}\cap U:\mathfrak{u}_\mathfrak{f})$$

von $2/Q_\mathfrak{f}$ als Nenner.

Wegen $W\cap\mathfrak{u} = W_\mathfrak{f}\cap\mathfrak{u} = \{\pm 1\}$ für die volle Einheitswurzelgruppe W von K ist

$$(\mathfrak{U}:\mathfrak{u}_\mathfrak{f})Q_\mathfrak{f} = (\mathfrak{U}:\mathfrak{u}W_\mathfrak{f}) = Q(\mathfrak{u}W:\mathfrak{u}W_\mathfrak{f}) = Qw/w_\mathfrak{f},$$

und man kann die Formel in die Gestalt

$$2^{\varkappa_\mathfrak{f}}Q\,\frac{h_k}{2}\,\frac{h^+}{w_\mathfrak{f}} = \prod_{\mathfrak{p}|\mathfrak{f}}\frac{\psi(\mathfrak{f}_\mathfrak{p})}{k(\mathfrak{f}_\mathfrak{p})}\,\frac{h_K}{w}$$

mit den Einheitwurzelanzahlen 2, w und $w_\mathfrak{f}$ von k, K und $\mathfrak{o}_\mathfrak{f}$ bringen.

Literatur

[1] Carl Friedrich Gauss, *Arithmetische Untersuchungen*, Hg. H. Maser, Berlin 1889, New York 1965.

[2] P. G. Lejeune-Dirichlet und R. Dedekind, *Vorlesungen über Zahlentheorie*, Vierte Ausgabe, Braunschweig 1893, Fünfte Ausgabe, New York 1968.

[3] Helmut Hasse, *Bericht über neuere Untersuchungen und Probleme aus der Theorie der algebraischen Zahlkörper*, Teil I. Jahresber. DMV 35 (1926), S. 1–55; Teil Ia Jahresber. DMV 36 (1927), S. 234–311 oder Zweite Ausgabe, Würzburg 1965.

[4] Rudolf Fricke, *Lehrbuch der Algebra*, 3. Band, Braunschweig 1928.

[5] Martin Eichler, *Quadratische Formen und orthogonale Gruppen*, Grundlehren 63, Zweite Ausgabe, Berlin 1952, 1974.

[6] Bartel L. v. d. Warden, *Algebra II*, Grundlehren 34, Vierte Ausgabe, Berlin 1959.

[7] Helmut Hasse, *Zahlentheorie*, Zweite Ausgabe, Berlin 1963.

[8] O. T. O'Meara, *Introduction to quadratic forms*, Grundlehren 117, Berlin 1963.

[9] Senon J. Borewicz und Igor R. Šafarevič, *Zahlentheorie*, Basel 1966.

[10] John S. Hsia, *Integral equivalence of vectors over depleted modular lattices on dyadic local fields*, Amer. J. Math. 90 (1968), S. 285–294.

[11] Irving Kaplansky, *Composition of binary quadratic forms*, Studia Math. 31 (1968), S. 523–530.

[12] Denise Legrand, *Formes quadratiques et algèbres quadratiques*, C. R. Acad. Sci. Paris 265 (1969), Sér. A, S. 764–767.

FACHBEREICH MATHEMATIK
JOHANNES-GUTENBERG-UNIVERSITÄT
Mainz

Eingegangen am 11.8.1978 (1093)