Ein allgemeines quadratisches Reziprozitätsgesetz in denjenigen algebraischen Zahlkörpern, worin 2 voll zerfällt.

Autor(en): **Skolem, Th.**

Objekttyp: **Article**

Zeitschrift: **Commentarii Mathematici Helvetici**

Band (Jahr): **5 (1933)**

PDF erstellt am: **24.04.2024**

Persistenter Link: https://doi.org/10.5169/seals-6664

Nutzungsbedingungen

Die ETH-Bibliothek ist Anbieterin der digitalisierten Zeitschriften. Sie besitzt keine Urheberrechte an den Inhalten der Zeitschriften. Die Rechte liegen in der Regel bei den Herausgebern.
Die auf der Plattform e-periodica veröffentlichten Dokumente stehen für nicht-kommerzielle Zwecke in Lehre und Forschung sowie für die private Nutzung frei zur Verfügung. Einzelne Dateien oder Ausdrucke aus diesem Angebot können zusammen mit diesen Nutzungsbedingungen und den korrekten Herkunftsbezeichnungen weitergegeben werden.
Das Veröffentlichen von Bildern in Print- und Online-Publikationen ist nur mit vorheriger Genehmigung der Rechteinhaber erlaubt. Die systematische Speicherung von Teilen des elektronischen Angebots auf anderen Servern bedarf ebenfalls des schriftlichen Einverständnisses der Rechteinhaber.

Haftungsausschluss

Alle Angaben erfolgen ohne Gewähr für Vollständigkeit oder Richtigkeit. Es wird keine Haftung übernommen für Schäden durch die Verwendung von Informationen aus diesem Online-Angebot oder durch das Fehlen von Informationen. Dies gilt auch für Inhalte Dritter, die über dieses Angebot zugänglich sind.

Ein Dienst der *ETH-Bibliothek*
ETH Zürich, Rämistrasse 101, 8092 Zürich, Schweiz, www.library.ethz.ch

http://www.e-periodica.ch

Ein allgemeines quadratisches Reziprozitätsgesetz in denjenigen algebraischen Zahlkörpern, worin 2 voll zerfällt.

Von Th. SKOLEM, Bergen.

Im folgenden betrachte ich in Zahlkörpern, worin 2 vollständig zerfällt, Jacobische Symbole, die in gewöhnlicher Art als Produkte von Legendreschen Symbolen definiert sein sollen. Dabei soll aber nicht wie gewöhnlich der Fall ausgeschlossen sein, daß ein Primfaktor l von 2 unter dem Strich (im „Nenner") auftritt. Weil jede zu l prime Zahl $\equiv 1$ (mod. l) ist, wenn 2 voll zerfällt, und also quadratischer Rest mod. l ist, so soll immer

$$\left(\frac{\alpha}{l}\right) = +1$$

gesetzt werden; dabei ist also natürlich α nicht teilbar durch l. Es sollen nämlich immer der „Zähler" und der „Nenner" der Jacobischen Symbole relativ prim sein. Nach der gemachten Vereinbarung hat dann das Symbol

$$\left(\frac{\alpha}{a}\right)$$

immer denselben Wert wie

$$\left(\frac{\alpha}{\bar{a}}\right),$$

wenn $\bar{a}$ der zu 2 prime Bestandteil von a ist, d. h. das Produkt derjenigen Primfaktoren von a, die in 2 nicht aufgehen. Man erkennt sehr leicht, daß die fundamentalen Sätze über die Jacobischen Symbole noch gültig bleiben, nämlich

1) $\left(\frac{\alpha}{ab}\right) = \left(\frac{\alpha}{a}\right)\left(\frac{\alpha}{b}\right)$ 2) $\left(\frac{\alpha\beta}{a}\right) = \left(\frac{\alpha}{a}\right)\left(\frac{\beta}{a}\right)$

3) Aus $\alpha \equiv \beta$ (mod. a) folgt $\left(\frac{\alpha}{a}\right) = \left(\frac{\beta}{a}\right)$.

Diese Erweiterung der Bedeutung des Jacobischen Symbols wird nun zuerst im absoluten Körper k gemacht. Ich setze, wenn $\left(\frac{a, k}{b}\right)$ solche Symbole im erweiterten Sinne sind,

$$\left(\frac{a, k}{b}\right)\left(\frac{b, k}{a}\right)(-1)^{\frac{\text{sign } a-1}{2}\,\frac{\text{sign } b-1}{2}} = (a, k, b).$$

Dann ist $(a, k, b) = (b, k, a)$ und $(a, k, bc) = (a, k, b)(a, k, c)$, wie man leicht konstatiert. Folgende Tatsachen können bemerkt werden:

Satz 1. *a) Sind a und b ungerade, so ist (a, k, b) bestimmt durch die Restklassen, wozu a und b gehören mod. 4.*

Beweis. Es ist für a und b ungerade

$$(a, k, b) = (-1)^{\frac{a-1}{2}\,\frac{b-1}{2}}.$$

b) Ist a teilbar durch genau 2^n, $n > 0$, b ungerade, so ist (a, k, b) bestimmt durch die Restklassen, wozu a und b bezw. mod. 2^{n+2} und 2^3 gehören.

Beweis. Es ist

$$(a, k, b) = \left(\frac{a, k}{b}\right)\left(\frac{b, k}{a}\right)(-1)^{\frac{\text{sign } a-1}{2}\,\frac{\text{sign } b-1}{2}} = \left(\frac{2, k}{b}\right)^n \left(\frac{a}{2^n}, k, b\right),$$

und $\left(\frac{2, k}{b}\right)$ ist bestimmt durch den Rest von b mod. 8, während nach a) $\left(\frac{a}{2^n}, k, b\right)$ bestimmt ist durch die Reste von $\frac{a}{2^n}$ und b mod. 4.

Weiter betrachte ich einen beliebigen Körper K vom Grade n, worin 2 voll zerfällt. Ich setze

$$(2) = \mathfrak{l}_1 \mathfrak{l}_2 \ldots \mathfrak{l}_n.$$

Die Zahlen aus K sollen durch kleine griechische Buchstaben, die Ideale aus K durch kleine deutsche Buchstaben bezeichnet werden, während absolut rationale Zahlen durch kleine lateinische Buchstaben bezeichnet werden.

Indem $\left(\frac{\alpha, K}{\mathfrak{p}}\right)$ das Jacobische Symbol im erweiterten Sinne ist, setze ich

$$\left(\frac{\alpha, K}{\mathfrak{p}}\right)\left(\frac{\beta, K}{\mathfrak{a}}\right)(-1)^{s\,\frac{\text{sign } \alpha-1}{2}\,\frac{\text{sign } \beta-1}{2}} = (\alpha, K, \beta)\ ^{1}).$$

---

[1]) Augenscheinlich ist wieder $(\alpha, K, \beta) = (\beta, K, \alpha)$ und $(\alpha, K, \beta\gamma) = (\alpha, K, \beta)(\alpha, K, \gamma)$.

Das Ziel dieses kleinen Aufsatzes ist nun zu zeigen, daß jedes Symbol (α, K, β) als ein Produkt von n „Komponent"symbolen (a, k, b) ausgedrückt werden kann, wobei die n Komponentsymbole den n Primfaktoren von 2 entsprechen. Wie dies zu verstehen ist, wird aus dem folgenden hervorgehen. In den Beweisen hierfür benutze ich keine höheren Mittel als die elementare Idealtheorie; freilich muß ich aber das quadratische Reziprozitätsgesetz für Zahlen, die prim zu 2 sind, als bekannt voraussetzen, nämlich [2])

$$\left(\frac{\alpha}{\beta}\right)\left(\frac{\beta}{\alpha}\right) = (-1)^{S\frac{\alpha-1}{2}\frac{\beta-1}{2} + S\frac{\operatorname{sign}\alpha-1}{2}\frac{\operatorname{sign}\beta-1}{2}}.$$

Bisweilen werde ich die bekannte „Nenner"transformationsformel

$$\left(\frac{a, K}{\mathfrak{a}}\right) = \left(\frac{a, k}{N\mathfrak{a}}\right)$$

benutzen, deren Richtigkeit in fast trivialer Weise beweisbar ist [3]). Daß diese Formel auch gültig bleibt bei der gemachten Erweiterung des Begriffes „Jacobisches Symbol" ist ohne weiteres klar.

Zuerst sollen 2 Hilfssätze bewiesen werden.

Hilfssatz 1. Es sei ω eine ganze primitive Zahl in K und $\equiv 1 \pmod{\mathfrak{l}_1^f}$, dagegen $\equiv 0 \pmod{\mathfrak{l}_i^f}$, wenn $i > 1$ ist. Dann ist $S\omega \equiv 1 \pmod{2^f}$.

Beweis. Die irreduzible Gleichung, der ω genügt, sei $f(\omega) = 0$. Sobald e hinreichend groß ist, gilt die Funktionenkongruenz

$$f(x) \equiv (x - a_1) \ldots (x - a_n) \pmod{2^e}$$

und zwar derart, [4]) daß für jedes i $\mathfrak{l}_i^f$ aufgeht in $\omega - a_i$. Also gelten dann die Kongruenzen

$$a_1 \equiv 1 \pmod{\mathfrak{l}_1^f}, \quad a_2 \equiv 0 \pmod{\mathfrak{l}_2^f}, \quad \ldots, \quad a_n \equiv 0 \pmod{\mathfrak{l}_n^f}$$

und also auch

$$a_1 \equiv 1, \quad a_2 \equiv a_3 \equiv \ldots \equiv a_n \equiv 0 \pmod{2^f}.$$

---

[2]) Vgl. *H. Hasse,* Bericht über neuere Untersuchungen und Probleme aus der Theorie der algebraischen Zahlkörper, Teil II, S. 77.

[3]) *H. Hasse,* Über das allgemeine Reziprozitätsgesetz etc., Journal für Math. 154, S. 107.

[4]) Vgl. *R. Fricke,* Lehrbuch der Algebra, Bd. 3, Kap. 2, § 14.

Folglich wird, da $e \geqq f$,

$$S\omega = a_1 + a_2 + \ldots + a_n \equiv 1 \pmod{2^f},$$

w. z. bw. w.

Hilfssatz 2. Es sei α eine ganze Zahl in K und für jedes i teilbar durch genau $\mathfrak{l}_i^{f_i}$ und $\equiv a_i$ mod. $\mathfrak{l}_i^{f_i+2}$. Dann ist[5]) $N\alpha \equiv \prod_i a_i \bmod. 2^{\sum_i f_i + 2}$.

Beweis. Zuerst zeige ich, daß der Satz gilt für jede Wahl der Zahlen a_i, falls er für eine solche gilt. Es sei nämlich für jedes i $a_i \equiv b_i \pmod{2^{f_i+2}}$. Dann ist b_i genau durch 2^{f_i} teilbar wie a_i, so daß man

$$a_i = 2^{f_i} a_i', \quad b_i = 2^{f_i} b_i', \quad a_i' \equiv b_i' \equiv \pm 1 \pmod 4$$

schreiben kann. Dann wird

$$\prod_i a_i' \equiv \prod_i b_i' \pmod 4,$$

woraus

$$\prod_i a_i = 2^{\sum_i f_i} \prod_i a_i' \equiv 2^{\sum_i f_i} \prod_i b_i' = \prod_i b_i \left(\bmod. 2^{\sum_i f_i + 2}\right).$$

Ich betrachte erstens eine primitive Zahl α. Die Gleichung für α in k sei $f(\alpha) \equiv 0$. Dann gilt für beliebiges e eine Funktionenkongruenz

$$f(x) \equiv (x - b_1) \ldots (x - b_n) \pmod{2^e},$$

und wenn e hinreichend groß ist[4]), so ist $\alpha - b_i$ teilbar durch $\mathfrak{l}_i^{f_i+2}$. Außerdem soll $e \geqq \sum_i f_i + 2$ gewählt werden. Dann ist

$$N\alpha \equiv \prod_i b_i \bmod. 2^e \quad \text{und also auch} \quad \bmod. 2^{\sum_i f_i + 2}.$$

Ist für jedes i dann $\alpha \equiv a_i \pmod{\mathfrak{l}_i^{f_i+2}}$, so ist $a_i \equiv b_i \pmod{2^{f_i+2}}$. Nach der zuerst gemachten Bemerkung folgt daraus $N\alpha \equiv \prod_i a_i \left(\bmod. 2^{\sum_i f_i + 2}\right)$.

Zweitens sei α imprimitiv. Dann kann man sicher eine primitive Zahl β finden, welche $\equiv \alpha \bmod. 2^{\sum_i f_i + 2}$ ist. Für jedes i ist dann auch $\beta \equiv a_i$

[5]) Überall im folgenden bedeuten $\prod_i$ und $\sum_i$ dasselbe wie $\prod_{i=1}^{n}$ bezw. $\sum_{i=1}^{n}$.

(mod. $\mathfrak{l}_i^{f_i+2}$), woraus man nach dem schon bewiesenen $N\beta \equiv \prod_i a_i \bmod. 2^{\sum f_i+2}$ bekommt. Da aber offenbar $N\alpha \equiv N\beta \pmod{2^{\sum f_i+2}}$, folgt $N\alpha \equiv \prod_i a_i \bmod. 2^{\sum f_i+2}$.

Satz 2. *Es seien α und β ganze Zahlen in K, relativ prim und prim zu 2. Es sei*

$$\alpha \equiv a_i, \quad \beta \equiv b_i \pmod{\mathfrak{l}_i^2}.$$

Dann ist

$$(\alpha, K, \beta) = \prod_i (a_i, k, b_i).$$

Beweis: Man kann n ganze und primitive Zahlen $\omega_1, \ldots, \omega_n$ in K finden derart, daß

$$\omega_i \equiv 1 \pmod{\mathfrak{l}_i^2}, \quad \omega_i \equiv 0 \pmod{\mathfrak{l}_j^2}, \text{ wenn } j \neq i.$$

Nach dem Hilfssatz 1 ist dann für alle i $S\omega_i \equiv 1 \pmod 4$. Außerdem hat man

$$\alpha \equiv a_1\omega_1 \ldots + a_n\omega_n, \quad \beta \equiv b_1\omega_1 + \ldots + b_n\omega_n \pmod 4;$$

denn jede dieser Kongruenzen gilt ja mod. $\mathfrak{l}_i^2$ für alle i, und deshalb wird

$$\frac{\alpha-1}{2} \equiv \sum_i \frac{a_i-1}{2}\omega_i, \quad \frac{\beta-1}{2} \equiv \sum_j \frac{b_j-1}{2}\omega_j \pmod 2$$

und

$$\frac{\alpha-1}{2}\frac{\beta-1}{2} \equiv \sum_h \frac{a_h-1}{2}\frac{b_h-1}{2}\omega_h^2 \pmod 2;$$

denn so oft $i \neq j$ ist, ist $\omega_i\omega_j \equiv 0 \pmod 4$. Nach dem Hilfssatze wird aber auch $S\omega_h^2 \equiv 1 \pmod 4$, und deshalb bekommt man

$$S\frac{\alpha-1}{2}\frac{\beta-1}{2} \equiv \sum_h \frac{a_h-1}{2}\frac{b_h-1}{2} \pmod 2.$$

Da

$$(\alpha, K, \beta) = (-1)^{S\frac{\alpha-1}{2}\frac{\beta-1}{2}} \quad \text{und} \quad (a, k, b) = (-1)^{\frac{a-1}{2}\frac{b-1}{2}},$$

so ist hierdurch Satz 2 bewiesen.

Satz 3. *Es seien α und β zwei relativ prime ganze Zahlen, $\beta \equiv 1$ (mod. 2), α teilbar durch genau $\mathfrak{l}_1^e$ und $\equiv 1 \left(\text{mod. } \frac{2}{\mathfrak{l}_1}\right)$. Ist $\alpha \equiv a_1$ (mod. $\mathfrak{l}_1^{e+2}$) und für jedes $i > 1 \equiv a_i$ (mod. $\mathfrak{l}_i^2$), während $\beta \equiv b_1$ ist mod. $\mathfrak{l}_1^3$ und für jedes $i > 1 \equiv b_i$ (mod. $\mathfrak{l}_i^2$), so ist*

$$(\alpha, K, \beta) = \prod_i (a_i, k, b_i).$$

Beweis: Zuerst soll der Satz bewiesen werden für eine beliebige Zahl β aber gewisse spezielle Zahlen α, nämlich

$$\alpha = \gamma^2 - \beta r,$$

wo r eine solche der Zahlen 1, 3, 5, 7 ist, daß $\beta r \equiv 1$ (mod. $\mathfrak{l}_1^3$) ist, während γ so bestimmt wird, daß

$$\gamma^2 - \beta r \text{ teilbar durch genau } \mathfrak{l}_1^e \text{ wird und } \gamma \equiv 0 \left(\text{mod. } \frac{2}{\mathfrak{l}_1}\right),$$

was offenbar alles stets möglich ist. Man kann auch γ prim zu β wählen, so daß auch α prim zu β wird.

Der zum Zahlenpaare (α, β) gehörende Signaturfaktor ist $= +1$; denn ist eine Konjugierte zu β negativ, so ist die entsprechende Konjugierte zu $\gamma^2 - \beta r$ augenscheinlich positiv. Also wird, wenn man bemerkt, daß

$$\left(\frac{\alpha, K}{r}\right) = \left(\frac{\gamma^2, K}{r}\right) = +1$$

ist,

$$(1) \quad (\alpha, K, \beta) = \left(\frac{\alpha, K}{\beta}\right)\left(\frac{\beta, K}{\alpha}\right) = \left(\frac{\gamma^2, K}{\beta}\right)\left(\frac{\gamma^2 r, K}{\alpha}\right) =$$
$$\left(\frac{r, K}{\alpha}\right)\left(\frac{\alpha, K}{r}\right) = \left(\frac{r, k}{N\alpha}\right)\left(\frac{N\alpha, k}{r}\right) = (r, k, N\alpha).$$

Nun ist $(N\alpha, k, r) = \left(\frac{2, k}{r}\right)^e \left(\frac{N\alpha}{2^e}, k, r\right)$ und nach dem Hilfssatze 2

$$\frac{N\alpha}{2^e} \equiv \frac{a_1}{2^e} a_2 a_3 \ldots a_n \text{ (mod. 4)},$$

so daß nach Satz 1

$$\left(\frac{N\alpha}{2^e},\ k,\ r\right) = \left(\frac{a_1}{2^e},\ k,\ r\right) \prod_{i=2}^{n} (a_i,\ k,\ r).$$

Da $r \equiv b_1 \pmod 8$, so ist

$$\left(\frac{a_1}{2^e},\ k,\ r\right) = \left(\frac{a_1}{2^e},\ k,\ b_1\right).$$

Wenn $i > 1$ ist, so hat man $a_i \equiv -b_i r \pmod 4$, woraus augenscheinlich

$$(a_i,\ k,\ r) = (a_i,\ k,\ b_i).$$

Aus den drei letzten Gleichungen folgt

$$\left(\frac{N\alpha}{2^e},\ k,\ r\right) = \left(\frac{a_1}{2^e},\ k,\ b_1\right) \prod_{i=2}^{n} (a_i,\ k,\ b_i).$$

Da aber $r \equiv b_1$ ist mod. 8, so ist $\left(\frac{2,\ k}{r}\right) = \left(\frac{2,\ k}{b_1}\right)$, so daß

$$(2)\quad (N\alpha,\ k,\ r) = \left(\frac{2,\ k}{r}\right)^e \left(\frac{N\alpha}{2^e},\ k,\ r\right) =$$

$$\left(\frac{2,\ k}{b_1}\right)^e \left(\frac{a_1}{2^e},\ k,\ b_1\right) \prod_{i=2}^{n} (a_i,\ k,\ b_i) = \prod_{i} (a_i,\ k,\ b_i).$$

Aus (1) und (2) folgt die Richtigkeit des Satzes in diesem Falle.

Um Satz 3 vollständig zu beweisen, braucht dann weiter nur folgendes gezeigt zu werden: Satz 3 gelte für $(\bar{\alpha},\ \beta)$, während α eine beliebige Zahl von der im Satze erwähnten Beschaffenheit ist. Dann gilt Satz 3 für $(\alpha,\ \beta)$.

Man hat, daß $\frac{\alpha}{\bar{\alpha}} = \frac{\delta}{\bar{\delta}}$ geschrieben werden kann, wo δ und $\bar{\delta}$ beide prim zu 2 und zu β sind. Ich setze $\bar{\alpha} \equiv \bar{a}_1 \pmod{\mathfrak{l}_1^{e+2}}$ und $\equiv \bar{a}_i \pmod{\mathfrak{l}_i^2}$ für $i > 1$, während $\alpha \equiv a_1$ bezw. a_i nach diesen Moduln ist. Ebenso schreibe ich δ bezw. $\bar{\delta}$ für jedes $i \equiv d_i$ bezw. $\bar{d}_i$ mod. $\mathfrak{l}_i^2$. Aus $\alpha\bar{\delta} = \bar{\alpha}\delta$ folgt

$$(\alpha\bar{\delta},\ K,\ \beta) = (\bar{\alpha}\delta,\ K,\ \beta),$$

und nach Satz 2 und der gemachten Annahme hat man

$$(\bar{\alpha}\delta, K, \beta) = (\bar{\alpha}, K, \beta)\ (\delta, K, \beta) = \prod_i (\bar{a}_i, k, b_i) \prod_i (d_i, k, b_i) = \prod_i (\bar{a}_i d_i, k, b_i).$$

Hieraus wieder nach Satz 2

$$(3) \quad (\alpha, K, \beta) = (\bar{\alpha}\delta, K, \beta)\,(\bar{\delta}, K, \beta) = \prod_i (\bar{a}_i d_i, k, b_i) \prod_i (\bar{d}_i, k, b_i).$$

Nun ist

$$\alpha\bar{\delta} \equiv a_1 \bar{d}_1 \text{ und } \bar{\alpha}\delta \equiv \bar{a}_1 d_1 \pmod{l_1^{e+2}},$$

wie man leicht findet. Aus der Gleichung $\alpha\bar{\delta} = \bar{\alpha}\delta$ folgt deshalb

$$a_1 \bar{d}_1 \equiv \bar{a}_1 d_1 \pmod{2^{e+2}},$$

woraus nach Satz 1

$$(a_1 \bar{d}_1, k, b_1) = (\bar{a}_1 d_1, k, b_1).$$

Ebenso hat man für $i > 1$

$$a_i \bar{d}_i \equiv \bar{a}_i d_i \pmod{4},$$

woraus nach Satz 1

$$(a_i \bar{d}_i, k, b_i) = (a_i \bar{d}_i, k, b_i).$$

Aus den beiden letzten Gleichungen folgt

$$\prod_i (a_i \bar{d}_i, k, b_i) = \prod_i (\bar{a}_i d_i, k, b_i),$$

woraus

$$(4) \qquad \prod_i (a_i, k, b_i) = \prod_i (\bar{a}_i d_i, k, b_i) \prod_i (\bar{d}_i, k, b_i).$$

Aus (3) und (4) folgt

$$(\alpha, K, \beta) = \prod_i (a_i, k, b_i).$$

Hierdurch ist Satz 3 vollständig bewiesen.

Satz 4. *Die ganzen Zahlen α und β seien relativ prim, α für jedes i teilbar durch genau $\mathfrak{l}_i^{e_i}$, β dagegen prim zu 2. Ist $\alpha \equiv a_i \pmod{\mathfrak{l}_i^{e_i+2}}$ und $\beta \equiv b_i \pmod{\mathfrak{l}_i^{g_i}}$, wo $g_i = 2$ oder $= 3$ ist, je nachdem $e_i = 0$ oder > 0 ist, so ist*

$$(\alpha, K, \beta) = \prod_i (a_i, k, b_i).$$

Beweis: Den Satz beweise ich zuerst für beliebiges β, aber nur gewisse α. Es sei nämlich für jede Zahl j der Reihe 1, 2, ... n α_j prim zu β und $\frac{2}{\mathfrak{l}_j}$, aber teilbar durch genau $\mathfrak{l}_j^{e_j}$. Dann ist $\alpha_1 \alpha_2 \dots \alpha_n$ eine spezielle Zahl[6]) α der im Satze erwähnten Art, und der Satz soll zuerst für das Zahlenpaar $(\prod_j \alpha_j, \beta)$ bewiesen werden.

Ich setze

$$\alpha_j \equiv a_{j,j} \pmod{\mathfrak{l}_j^{e_j+2}} \text{ und } \equiv a_{j,i} \pmod{\mathfrak{l}_i^2}, \text{ wenn } i \neq j.$$

Nun ist

$$\left(\prod_j \alpha_j, K, \beta\right) = \prod_j (\alpha_j, K, \beta)$$

und nach Satz 3 für alle j

$$(\alpha_j, K, \beta) = \prod_i (a_{ji}, k, b_i);$$

denn für alle i ist ja $\beta \equiv b_i \pmod{\mathfrak{l}_i^2}$ und falls $e_j > 0$ ist, β sogar $\equiv b_j \pmod{\mathfrak{l}_j^3}$.

Also wird

$$(5) \qquad \left(\prod_j \alpha_j, K, \beta\right) = \prod_j \prod_i (a_{ji}, k, b_i) = \prod_i \left(\prod_j a_{ji}, k, b_i\right).$$

Außerdem ist

$$\prod_{j \neq i} \alpha_j \equiv \prod_{j (\neq i)} a_{ji} \pmod{\mathfrak{l}_i^2},$$

[6]) Ist die Zahl der Idealklassen in K gleich 1, so kann freilich jede Zahl α in dieser Form geschrieben werden.

woraus, da α_i teilbar ist durch $\mathfrak{l}_i^{e_i}$ und $\equiv a_{ii}$ mod. $\mathfrak{l}_i^{e_i+2}$ ist,

$$\prod_j \alpha_j \equiv \prod_j a_{ji} \pmod{\mathfrak{l}_i^{e_i+2}}. \tag{6}$$

Aus (5) und (6) folgt die Wahrheit des Satzes in diesem Falle.

Danach soll eine beliebige Zahl α der im Satz erwähnten Art betrachtet werden. Ich setze der Kürze halber $\prod_j \alpha_j = \bar{\alpha}$, $\prod_j a_{ji} = \bar{a}_i$, und man hat

$$\frac{\alpha}{\bar{\alpha}} = \frac{\delta}{\bar{\delta}},$$

wo δ und $\bar{\delta}$ prim zu 2 und β sind, und es soll für jedes i

$$\delta \equiv d_i, \ \bar{\delta} \equiv \bar{d}_i \pmod{\mathfrak{l}_i^2}$$

sein. Da $\alpha\bar{\delta} = \bar{\alpha}\delta$ ist, bekommt man unter Benutzung des schon bewiesenen

$$(\alpha\bar{\delta}, K, \beta) = (\bar{\alpha}\delta, K, \beta) = (\bar{\alpha}, K, \beta)(\delta, K, \beta) =$$
$$\prod_i (\bar{a}_i, k, b_i) \prod_i (d_i, k, b_i) = \prod_i (\bar{a}_i d_i, k, b_i)$$

und

$$(\alpha, K, \beta) = (\bar{\alpha}\delta, K, \beta)(\bar{\delta}, K, \beta) = \prod_i (\bar{a}_i d_i, k, b_i) \prod_i (\bar{d}_i, k, b_i). \tag{7}$$

Nun ist

$$\alpha\bar{\delta} \equiv a_i \bar{d}_i \text{ und } \bar{\alpha}\delta \equiv \bar{a}_i d_i \pmod{\mathfrak{l}_i^{e_i+2}}$$

und also

$$a_i \bar{d}_i \equiv \bar{a}_i d_i \pmod{2^{e_i+2}},$$

woraus nach Satz 1

$$(a_i \bar{d}_i, k, b_i) = (\bar{a}_i d_i, k, b_i)$$

oder

$$(a_i, k, b_i) = (\bar{a}_i d_i, k, b_i)(\bar{d}_i, k, b_i). \tag{8}$$

Aus (7) und (8) folgt wiederum

$$(\alpha, K, \beta) = \prod_i (a_i, k, b_i).$$

Hierdurch ist Satz 4 bewiesen.

Satz 5. *Die ganzen Zahlen α und β seien relativ prim und für jedes i α genau teilbar durch $\mathfrak{l}_i^{e_i}$, β teilbar durch genau $\mathfrak{l}_i^{f_i}$. Weiter sei für jedes i $\alpha \equiv a_i$ (mod. $\mathfrak{l}_i^{g_i}$), $\beta \equiv b_i$ (mod. $\mathfrak{l}_i^{h_i}$), wobei $g_i = e_i + 2$ oder $= 3$ ist, je nachdem $f_i = 0$ oder > 0 ist, und ebenso $h_i = f_i + 2$ oder $= 3$, je nachdem $e_i = 0$ oder > 0 ist. Dann gilt die Gleichung*

$$(\alpha, K, \beta) = \prod_i (a_i, k, b_i).$$

Beweis: Indem β beliebig ist, beweise ich den Satz zuerst für gewisse spezielle α, nämlich

$$\alpha = \gamma^2 - \beta\xi.$$

So oft $e_i > 0$ sein soll, wird ξ so gewählt, daß

$$\beta\xi \equiv 1 \pmod{\mathfrak{l}_i^3} \tag{9}$$

wird, und danach γ so bestimmt, daß α teilbar durch genau $\mathfrak{l}_i^{e_i}$ wird. Ist $f_i > 0$, setze man $\gamma \equiv 1$ (mod. $\mathfrak{l}_i$); dann wird ja $e_i = 0$. Soll endlich $e_i = 0$ sein, indem auch $f_i = 0$ ist, so setze man $\gamma \equiv 0$ (mod. $\mathfrak{l}_i$). Außerdem kann man ξ total positiv und überhaupt prim zu 2 wählen. Dann hat man, weil der Signaturfaktor offenbar $= +1$ wird,

$$(\alpha, K, \beta) = \left(\frac{\alpha, K}{\beta}\right)\left(\frac{\beta, K}{\alpha}\right) = \left(\frac{\xi, K}{\alpha}\right) = \left(\frac{\xi, K}{\alpha}\right)\left(\frac{\alpha, K}{\xi}\right) = (\alpha, K, \xi). \tag{10}$$

Nach Satz 4 ist nun

$$(\alpha, K, \xi) = \prod_i (a_i, k, x_i), \tag{11}$$

wenn $\xi \equiv x_i$ mod. $\mathfrak{l}_i^3$ ist, wenn $e_i > 0$, und mod. $\mathfrak{l}_i^2$ sonst. Nun wird aber nach (9) $b_i x_i \equiv 1$ (mod. 8), so oft $e_i > 0$ ist, woraus folgt $(a_i, k, x_i) = (a_i, k, b_i)$. Ist $e_i = f_i = 0$, so ist $a_i \equiv -b_i x_i$ (mod. 4), woraus $(a_i, k, x_i) = (a_i, k, b_i)$. Es bleibt der Fall $f_i > 0$. Dann ist $\beta \equiv b_i$ mod. $\mathfrak{l}_i^{f_i+2}$ und

also in jedem Falle mod. $\mathfrak{l}_i^8$. Weiter ist $\gamma \equiv 1 \pmod{\mathfrak{l}_i}$, woraus bekanntlich $\gamma^2 \equiv 1 \pmod{\mathfrak{l}_i^8}$. Da außerdem $\alpha \equiv a_i \bmod \mathfrak{l}_i^3$, bekommt man

$$a_i \equiv 1 - b_i x_i \pmod 8,$$

und b_i ist eine gerade Zahl, nämlich teilbar durch 2^{f_i}. Nun wird

$$(a_i, k, b_i) = \left(\frac{2, k}{a_i}\right)^{f_i} \left(a_i, k, \frac{b_i}{2^{f_i}}\right).$$

Ist $f_i \geqq 3$, so ist $a_i \equiv 1 \pmod 8$, woraus $(a_i, k, b_i) = 1 = (a_i, k, x_i)$. Ist $f_i = 2$, so ist $a_i \equiv 1 \pmod 4$, woraus wiederum $(a_i, k, b_i) = 1 = (a_i, k, x_i)$. Ist endlich $f_i = 1$, so hat man

$$\text{entweder } \frac{b_i x_i}{2} \equiv 1 \quad \text{oder} \quad \equiv -1 \pmod 4.$$

Im ersten Falle ist $a_i \equiv -1 \pmod 8$ und deshalb

$$(a_i, k, b_i) = \left(a_i, k, \frac{b_i}{2}\right) = (a_i, k, x_i).$$

Im zweiten Falle ist $a_i \equiv 3 \pmod 8$, woraus

$$(a_i, k, b_i) = -\left(a_i, k, \frac{b_i}{2}\right) = (a_i, k, x_i).$$

Man hat also für alle i, daß $(a_i, k, x_i) = (a_i, k, b_i)$ ist. Dies in Verbindung mit (10) und (11) zeigt die Richtigkeit von Satz 5 für die speziellen α.

Um die Allgemeingültigkeit des Satzes zu zeigen gehe ich in derselben Weise wie früher vor. Der Satz sei also gültig für $(\bar{\alpha}, \beta)$, und α sei eine beliebige Zahl der im Satze erwähnten Beschaffenheit. Ich setze

$$\frac{\alpha}{\bar{\alpha}} = \frac{\delta}{\bar{\delta}},$$

wo δ und $\bar{\delta}$ prim zu 2β sind. Weiter sollen δ und $\bar{\delta} \equiv d_i$ bezw. $\bar{d}_i \bmod \mathfrak{l}_i^{t_i}$ sein, wo $t_i = 2$ oder $= 3$ ist, je nachdem $f_i = 0$ oder > 0 ist. Wie früher hat man

$$(\alpha, K, \beta) = (\bar{\alpha}, K, \beta)(\delta, K, \beta)(\bar{\delta}, K, \beta),$$

und nach der gemachten Voraussetzung und nach Satz 4 erhält man

$$(12) \qquad (\alpha, K, \beta) = \prod_i (\bar{a}_i\, d_i, k, b_i) \cdot \prod_i (\bar{d}_i, k, b_i).$$

Andererseits folgt aus der Gleichung $\alpha\bar{\delta} = \bar{\alpha}\,\delta$, daß wenn zuerst die i, für welche $f_i = 0$ ist, betrachtet werden

$$a_i\,\bar{d}_i \equiv \bar{a}_i\, d_i \pmod{2^{e_i+2}};$$

denn $\alpha\bar{\delta} \equiv a_i\bar{d}_i$ und $\bar{\alpha}\delta \equiv \bar{a}_i\, d_i \bmod \mathfrak{l}_i^{e_i+2}$, wie leicht einzusehen. Da $a_i\bar{d}_i$ und $\bar{a}_i d_i$ teilbar sind durch 2^{e_i}, aber nicht 2^{e_i+1}, so folgt nach Satz 1, daß

$$(a_i\bar{d}_i, k, b_i) = (\bar{a}_i d_i, k, b_i),$$

woraus

$$(13) \qquad (a_i, k, b_i) = (\bar{a}_i d_i, k, b_i)(\bar{d}_i, k, b_i).$$

Ist $f_i > 0$, so hat man $\alpha\bar{\delta} \equiv a_i\bar{d}_i$ und $\bar{\alpha}\delta \equiv \bar{a}_i d_i \bmod \mathfrak{l}_i^3$, woraus

$$a_i\bar{d}_i \equiv \bar{a}_i d_i \pmod 8;$$

außerdem sind $a_i\bar{d}_i$ und $\bar{a}_i d_i$ ungerade.
Aber dann ist offenbar wiederum

$$(a_i\bar{d}_i, k, b_i) = (\bar{a}_i d_i, k, b_i)$$

oder

$$(14) \qquad (a_i, k, b_i) = (\bar{a}_i d_i, k, b_i)(\bar{d}_i, k, b_i).$$

Aus (12), (13) und (14) folgt die Richtigkeit des Satzes 5, der hierdurch vollständig bewiesen ist.

Beispiel: Im Körper $k(\sqrt{-7})$ ist $2 = \lambda_1\lambda_2$, wobei

$$\lambda_1 = \frac{1+\sqrt{-7}}{2}, \quad \lambda_2 = \frac{1-\sqrt{-7}}{2},$$

sind. Es wird z. B.

$$\alpha = \frac{-5+3\sqrt{-7}}{2}, \quad \beta = 1+2\sqrt{-7}$$

gewählt. Hier ist $\beta \equiv 1 \pmod 2$; dagegen ist α prim zu λ_2, aber teilbar durch λ_1, indem

$$\alpha = (2+\sqrt{-7})\,\lambda_1$$

ist. Man findet

$$\lambda_1^3 = \frac{-5-\sqrt{-7}}{2}, \quad \lambda_2^{2i} = \frac{-3-\sqrt{-7}}{2}.$$

Mod. λ_1^3 sind dann

$$\alpha \equiv \frac{-5-15}{2} = -10 \equiv 6 \text{ und } \beta \equiv 1 - 10 = -9 \equiv 7.$$

Mod. λ_2^2 sind

$$\alpha \equiv \frac{-5-9}{2} = -7 \equiv 1 \text{ und } \beta \equiv 1 - 6 = -5 \equiv 3.$$

Deshalb wird (dies folgt schon aus Satz 3 oben)

$$(\alpha, k(\sqrt{-7}), \beta) = (6, k, 7)(1, k, 3).$$

Nun ist $(1, k, 3) = 1$, während

$$(6, k, 7) = \left(\frac{2, k}{7}\right)(3, k, 7) = +1 \cdot -1 = -1.$$

Also, da der Signaturfaktor in einem total imaginären Körper immer $= +1$ ist,

$$\left(\frac{\alpha, k(\sqrt{-7})}{\beta}\right)\left(\frac{\beta, k(\sqrt{-7})}{\alpha}\right) = -1.$$

Nun findet man leicht, daß $\alpha \equiv 4$ ist mod. β; also ist $\left(\frac{\alpha, k(\sqrt{-7})}{\beta}\right) = +1$. Weiter ist nach der gemachten Vereinbarung

$$\left(\frac{\beta, k(\sqrt{-7})}{\alpha}\right) = \left(\frac{\beta, k(\sqrt{-7})}{2+\sqrt{-7}}\right).$$

Mod. $2+\sqrt{-7}$ ist aber $\beta \equiv -3$ und $\left(\frac{-3, k(\sqrt{-7})}{2+\sqrt{-7}}\right) = \left(\frac{-3, k}{11}\right) = \left(\frac{11, k}{3}\right) = \left(\frac{-1, k}{3}\right) = -1$. Dadurch ist das obige Ergebnis bestätigt.

(Eingegangen den 15. November 1932.)