Werk

Titel: Journal für die reine und angewandte Mathematik
Verlag: de Gruyter
Jahr: 1937
Kollektion: Mathematica
Digitalisiert: Niedersächsische Staats- und Universitätsbibliothek Göttingen
Werk Id: PPN243919689_0176
PURL: http://resolver.sub.uni-goettingen.de/purl?PPN243919689_0176

LOG Id: LOG_0011
LOG Titel: Zur Gaußschen Kompositionstheorie der binären quadratischen Formen.
LOG Typ: article

Übergeordnetes Werk

Werk Id: PPN243919689
PURL: http://resolver.sub.uni-goettingen.de/purl?PPN243919689

Terms and Conditions

Contact

Niedersächsische Staats- und Universitätsbibliothek Göttingen
Georg-August-Universität Göttingen
Platz der Göttinger Sieben 1
37073 Göttingen
Germany
Email: gdz@sub.uni-goettingen.de

Zur Gaußschen Kompositionstheorie der binären quadratischen Formen.

Von *S. Lubelski* in Warschau.

Die Gaußsche Kompositionstheorie der binären quadratischen Formen verläuft bekanntlich parallel mit der Dedekind-Hilbertschen Idealklassentheorie quadratischer Körper [1]). Demnach scheint die erstere überflüssig zu sein. Doch ist sie als Beweismethode für die Theorie der binären quadratischen Formen $f(x, y)$ mit ganzen algebraischen Koeffizienten von Bedeutung. Sie gibt uns nämlich die Möglichkeit, in natürlicher und verhältnismäßig klarer Weise die Untergruppe g der gesamten Idealklassengruppe G, die durch $f(x, y)$ gebildet wird, hervorzuheben und oft die Ordnung H von g zu berechnen. In einer früheren Arbeit [2]) habe ich nämlich den folgenden Satz bewiesen:

Satz 1. *Es sei* $K(\sqrt{-q})$, $q \neq 2$ *Primzahl, ein imaginär-quadratischer Körper mit ungerader Klassenzahl,* $D > 2$ *eine natürliche Zahl, die für* $q = 1$ *größer als* 12 *ist und für welche* $D' = \frac{D}{4}$ *eine ganze, durch keine Quadratzahl des Körpers* $K(\sqrt{-q})$ *teilbare Zahl ist; ferner sei* h *die Klassenzahl der binären quadratischen Formen der Determinante* D, h' *die Klassenzahl der binären quadratischen Formen der Determinante* $-qD$ *im Körper der rationalen Zahlen. Dann gilt:*

Die Klassenzahl H *der binären quadratischen Formen der Determinante* D, *deren Koeffizienten ganze Zahlen des Körpers* $K(\sqrt{-q})$ *sind, ist* $H = \frac{hh'}{2}$ *für* $q \geqq 3$. *Ist* $q = 1$, *so ist* $H = hh'$ *oder* $2hh'$, *je nachdem* $x^2 - D'y^2 = -1$ *in ganzen rationalen Zahlen lösbar ist oder nicht.*

Die Herglotzsche Formel für die Ordnung H_1 von G ergibt für $D \geqq 12$

$$H_1 = \frac{hh'h_1}{2},$$

wo h_1 die Klassenzahl von $K(\sqrt{-q})$ bezeichnet [3]). Im Falle $h_1 = 1$ decken sich offenbar beide Formeln. Im allgemeinen sind sie aber wesentlich verschieden. Unsere Formel ist nämlich nur von *zwei* Parametern abhängig, die Herglotzsche dagegen von *drei*. In gewissen Fällen, z. B. für $(h_1, \frac{1}{2}hh') = 1$, erhält man mittels eines Furtwänglerschen

[1]) Dies war die Ursache dafür, daß man sich nicht mit der Gaußschen Kompositionstheorie beschäftigt hatte.

[2]) S. Lubelski, Über Klassenzahlrelationen quadratischer Formen in quadratischen Körpern, Journ. f. d. r. u. a. Math. **174** (1935), S. 160—184.

[3]) Man sieht also schon aus dieser Formel, wie auch aus Satz 1, daß unsere Bemerkung in [2]), S. 160: *die Klassenzahl* H *eines algebraischen Körpers . . ., der durch Zusammensetzung von* m *quadratischen Körpern* K_g $(g = 1, 2, \ldots, m)$ *entsteht . . ., ist durch das Produkt der Klassenzahlen* $h_1 h_2 \cdots h_m$ *teilbar*, offenbar bis auf einen Faktor $\frac{1}{2^t}$ gedacht ist.

Satzes (vgl. Satz 3 von [2])) aus einer Formel die andere. Um das Verhältnis der Formeln von H und H_1 ausführlich zu beleuchten, brauchen wir eine rein arithmetische Interpretation der Herglotzschen Formel, die wir nur für ungerades H_1 geben. Daraus erhalten wir in § 1 mit elementaren Mitteln einerseits eine Abschätzung der Herglotzschen Formel für relativ quadratische Körper mit ungerader Klassenzahl, andererseits Sätze über die *simultane Darstellbarkeit von rationalen Primzahlen durch binäre quadratische Formen.* Die genannten Formeln sind also für die Verteilung der Primzahlen von Bedeutung.

In § 2 geben wir auf Grund der Gaußschen Kompositionstheorie den (längst gesuchten) rein arithmetischen (also ohne Zuhilfenahme des Begriffes der reellen Zahl geführten) Beweis für die Existenz von nichttrivialen ganzen rationalen Lösungen der Pellschen Gleichung $x^2 - Dy^2 = 1$. Zugleich ergibt sich ein einfacher Beweis einer merkwürdigen Petrschen Verallgemeinerung des letzteren Satzes.

§ 1.

Satz 2. *Ist K ein über $K(\sqrt{-q})$ relativ quadratischer Körper, so entspricht jeder Idealklasse C aus K eindeutig ein System von drei ganzzahligen Formen $\{F_i\}$, deren Diskriminanten den Diskriminanten der quadratischen Unterkörper paarweise gleich sind. Sind C und $\overline{C}$ zwei Idealklassen, denen die Formensysteme $\{F_i\}$, $\{\overline{F}_i\}$ entsprechen, so entspricht dem Produkte $C\overline{C}$ das Formensystem $\{F_i\overline{F}_i\}$. Ist die Klassenzahl H_1 von K ungerade, so ist die genannte Zuordnung umkehrbar eindeutig.*

Beweis. Es seien $K(\sqrt{d_i})$ sämtliche quadratischen Körper, die zu K gehören, Δ_i ihre Diskriminanten. Ist j ein zur Idealklasse C von K gehöriges Ideal, so bilden die ganzen zu j und $K(\sqrt{d_i})$ gehörigen Zahlen ein Ideal j_i. Die ganzzahligen binären quadratischen Formen, die j_i entsprechen, ordnen wir der Idealklasse C zu. Nun ist $j_i = js_ij$, wo s_ij aus j nach Ausführung einer entsprechenden, eindeutig bestimmten Permutation s_i der galoisschen Gruppe von K entsteht. Sind also C und $\overline{C}$ zwei Idealklassen aus K, so entspricht der Idealklasse $C\overline{C}$ das Formensystem $\{F_i\overline{F}_i\}$, wenn nur $\{F_i\}$ bzw. $\{\overline{F}_i\}$ der Idealklasse C bzw. $\overline{C}$ entspricht. Mithin läßt sich die Eindeutigkeit der Zuordnung leicht beweisen. Denn sind j und $\bar{j}$ zwei zu C gehörige Ideale, so folgt aus $j = l\bar{j}$, wo l eine Zahl des Körpers K ist, daß $j(s_ij) = l(s_il)\cdot\bar{j}(s_i\bar{j})$ ist, wo $l(s_il)$ zu $K(\sqrt{d_i})$ gehört. Also gehören $j(s_ij)$ und $\bar{j}(s_i\bar{j})$ zu derselben Klasse von $K(\sqrt{d_i})$.

Schwieriger ist zu beweisen, ob die genannte Zuordnung eindeutig umkehrbar ist. Dazu müssen wir H_1 als ungerade voraussetzen. Sind nämlich C und $\overline{C}$ zwei Idealklassen, denen dasselbe System $\{F_i\}$ entspricht, so ergibt die Idealklasse $C\overline{C}^{-1}$ das Hauptsystem, d. h. das System, das aus den Hauptformen von $K(\sqrt{d_i})$ besteht. Bezeichnet $\mathfrak{a}$ ein beliebiges zu $\overline{C}C^{-1}$ gehöriges Ideal, so ergibt also $\mathfrak{a}s_i\mathfrak{a}$ eine Zahl aus $K(\sqrt{d_i})$. Demnach gehört $s_i\mathfrak{a}$ zur Klasse $\overline{C}^{-1}C$. Da $\mathfrak{a}(s_1\mathfrak{a})(s_2\mathfrak{a})(s_3\mathfrak{a}) = N(\mathfrak{a})$ ist, so ist $\overline{C}^{-1}C$ ambig und mithin $\overline{C}^{-1}C$ die Einheitsklasse, da H_1 ungerade ist.

Folgerung. *Die Anzahl H_1 der Idealklassen von K ist ein Teiler des Produktes der Idealklassen von $K(\sqrt{d_i})$, sofern H_1 ungerade ist.*

Der Beweis ergibt sich unmittelbar aus der Tatsache, daß sämtliche Systeme $\{F_i\}$ eine Gruppe $\mathfrak{G}$ bilden. Diejenigen Systeme, die den Idealklassen von K entsprechen, bilden also eine Untergruppe von $\mathfrak{G}$.

Satz 3. *Eine rationale Primzahl p sei durch die ganzzahligen Formen*

$$f(x, y) = ax^2 + bxy + cy^2, \quad f_1(x, y) = a_1x^2 + b_1xy + c_1y^2$$

gleichzeitig darstellbar. Die Diskriminanten $d = b^2 - 4ac$, $d_1 = b_1^2 - 4a_1c_1$ seien bis auf 4 quadratfrei, $(p, 4dd_1) = 1$, und die Klassenzahl H_1 von $K(\sqrt{d}, \sqrt{d_1})$ sei ungerade. Dann stellen die Formen $f(x, y)$, $f_1(x, y)$ unendlich viele Primzahlen dar, und die Menge dieser Primzahlen ist von positiver Dichte.

Beweis. Es bezeichne $\mathfrak{p}$ einen Primidealteiler von p und C die Klasse, zu der $\mathfrak{p}$ gehört. Offenbar ist p nach den Voraussetzungen des Satzes in $K(\sqrt{d})$ wie auch in $K(\sqrt{d_1})$ zerlegbar. Demnach ist $p = \mathfrak{p}\mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3$, wo $\mathfrak{p}, \mathfrak{p}_1, \mathfrak{p}_2, \mathfrak{p}_3$ Primideale ersten Grades sind. Der Klasse C, zu der $\mathfrak{p}$ gehört, entspricht also nach Satz 2 ein System von Formen, zu dem $f(x, y)$ und $f_1(x, y)$ gleichzeitig gehören. Nach einem Furtwänglerschen Satze enthält C unendlich viele Primideale ersten Grades, deren Normen nach Satz 2 durch die Formen $f(x, y)$, $f_1(x, y)$ gleichzeitig darstellbar sind. Nach dem Furtwänglerschen Satze beträgt die Dichte der Primzahlen ersten Grades, die zu C gehören, $\frac{1}{4H_1}$.

Folgerung. *Bei den Voraussetzungen der Sätze 1 und 2 ist die Anzahl der Systeme $\{F_i\}$ (wo F_1 eine Hauptform mit negativer Diskriminante bezeichnet), die gleichzeitig unendlich viele Primzahlen darstellen, $H = \frac{1}{2}\frac{H_1}{h_1}$* (dies ist also auch die Anzahl der Systeme, die keine in der Diskriminante von K nicht enthaltenen Primzahlen darstellen).

Beweis. Die Anzahl der Systeme $\{f_i\}$, die den Idealklassen nach Satz 1 und 2 entsprechen, beträgt $\frac{1}{2}\frac{H_1}{h_1} = H$. Die Formen dieser Systeme stellen also unendlich viele Primzahlen dar. Nun ist eine Form eines solchen Systems der Hauptform des imaginärquadratischen Körpers $K(\sqrt{-q})$ gleich.

Bemerkung. Der Satz 3 gibt uns die Möglichkeit, die Systeme $\{F_i\}$ effektiv aufzufinden, sogar allgemein. Z. B. ist im relativ quadratischen Körper $K(\sqrt{3}, \sqrt{-5})$ die Klassenzahl nach Herglotz gleich 2. Da

$$47 = 3 \cdot 3^2 + 5 \cdot 2^2 = 2 \cdot 2^2 + 2 \cdot 2 \cdot 3 + 3 \cdot 3^2$$

ist, so sind nur die Formensysteme

$$\{\pm(x^2 - 3y^2),\ x^2 + 5y^2,\ x^2 + 15y^2\}, \qquad \{\pm(x^2 - 3y^2),\ 2x^2 + 2xy + 3y^2,\ 3x^2 + 5y^2\}$$

möglich und nur diese stellen also gleichzeitig unendlich viele Primzahlen dar. Demnach ist die Anzahl der binären quadratischen Formen der Determinante 12 mit Koeffizienten aus dem Körper $K(\sqrt{-5})$ gleich 1.

Bemerkung. Aus den Sätzen 1, 2 und aus der Herglotzschen Formel erhält man leicht, daß $H_1 = \frac{hh'h_1}{2}$. Dagegen folgt dies allein aus der Herglotzschen Formel nicht unmittelbar.

§ 2.

Satz 4 (Arithmetischer Beweis der Lösbarkeit der Pellschen Gleichung). *Die Gleichung $x^2 - Dy^2 = 1$, wo D eine natürliche quadratfreie Zahl bezeichnet, ist in natürlichen Zahlen x, y lösbar.*

Beweis. I. Wäre die Gleichung

$$x^2 - Dy^2 = d, \quad d \mid D \tag{1}$$

in natürlichen Zahlen lösbar, so würde sich aus

$$dx_1 = x, \quad dx_1^2 - D_1 y^2 = 1, \qquad D_1 = \frac{D}{d},$$

die Gleichung

$$(dx_1^2 + D_1 y^2)^2 - D(2y^2 x_1^2)^2 = (dx_1^2 - D_1 y^2)^2 = 1$$

ergeben. Wir können also annehmen, daß auch die Gleichung (1) nicht lösbar ist.

II. Demnach kann man leicht eine untere Grenze für die Anzahl der ambigen Formen der Determinante $4D$ angeben. Nach einem Gaußschen Satze kann jede ambige Form in die Gestalt $ax^2 + a\varrho xy + cy^2$ $(\varrho = 0, 1)$ transformiert werden [4]). Sind die verschiedenen Formen

$$ax^2 + a\varrho\, xy + cy^2, \qquad a_1 x^2 + a_1 \varrho_1 xy + c_1 y^2 \qquad (\varrho, \varrho_1 = 0, 1)$$

der Determinante $4D$ zueinander äquivalent, so ist für gewisse ganze rationale Zahlen u, V

$$a_1 = au^2 + a\varrho uV + V^2, \quad aa_1 = U^2 - DV^2, \quad U = au + \frac{a\varrho}{2} V.$$

Da D quadratfrei ist, so muß $(a, a_1) | (U, V)$ sein. Mithin ist d durch $x^2 - Dy^2$ darstellbar, wobei $d = \frac{aa_1}{(a, a_1)^2}$, $d | D$ ist. Nach I ist dies nur dann möglich, wenn $a_1 = -\frac{DV^2}{a}$ ist. Zwei ambige Formen $ax^2 + a\varrho xy + cy^2$ mit positiven ersten Koeffizienten sind also nicht äquivalent, wenn nur $a \neq a_1$ ist. Nun erhalten wir für $\varrho = 1$ und $a = 2\bar{a}$

$$(2\bar{a})^2 - 4\,(2\bar{a})\,c = 4D,$$

also $\bar{a}^2 - 2\bar{a}c = D$. Da c ungerade ist, so muß gelten:

$$D \equiv -1 \pmod 4 \text{ für ungerades } \bar{a}, \quad 4 | D \text{ für gerades } \bar{a}.$$

$4 | D$ ist unmöglich. Bezeichnet v die Anzahl der ungeraden Primteiler von D, so beträgt also die Anzahl der ambigen Formen für $D \equiv 1 \pmod 4$ mindestens 2^v, für $D \equiv 2, -1 \pmod 4$ mindestens 2^{v+1} (für $D \equiv -1 \bmod 4$ ist zugleich $\varrho = 0, 1$ möglich).

III. Jeder binären quadratischen Form $ax^2 + bxy + cy^2$ der Determinante $4D$ ordnen wir ihre Charaktere $\left(\frac{m}{p}\right)$, $(-1)^{t(m)}$ zu, wo m eine durch $ax^2 + bxy + cy^2$ darstellbare Zahl bezeichnet, $t(m)$ ein gewisses Polynom, $(m, 2D) = 1$ und n ungerader Primteiler von D ist. Sie sind nur von der Form $ax^2 + bxy + cy^2$ abhängig; dabei ist ihre Anzahl für $D \equiv 1 \pmod 4$ gleich v, für andere D gleich $v + 1$ [5]). Die binären quadratischen Formen, denen dasselbe Charakterensystem entspricht, bilden ein Geschlecht. Diejenigen, bei denen die Charaktere sämtlich gleich 1 sind, bilden das Hauptgeschlecht. Offenbar gehört das Quadrat einer beliebigen Form zum Hauptgeschlecht. Nach einem Gaußschen Satze [6]) ist auch umgekehrt jede Form des Hauptgeschlechts Quadrat einer anderen Form. Durchläuft also C_i^2 $(i = 1, 2, \ldots)$ sämtliche verschiedenen Quadrate der Formen der Diskriminante $4D$, so ist jede Form derselben Diskriminante einer Form αC_i gleich, wo α^2 die Einheitsform ist. Bezeichnet also H die Klassenzahl der Determinante $4D$, A die Anzahl der ambigen Formen und h die Anzahl der Formen des Haupt-

[4]) Vgl. z. B. E. Cahen, Theorie des Nombres II, Paris 1924, S. 324—326.

[5]) Vgl. z. B. Cahen, a. a. O. [4]) S. 397—399.

[6]) Vgl. z. B. Dirichlet-Dedekind, Vorlesungen über Zahlentheorie (1894), §§ 155—158, oder H. Hasse, Elementarer Beweis des Hauptsatzes über ternäre quadratische Formen mit rationalen Koeffizienten, Journ. f. d. r. u. a. Math. **172** (1935), S. 129—132.

geschlechtes, so ist $H = Ah$. Andererseits ist $H = gh$, wo g die Anzahl der Geschlechter von $4D$ bedeutet. Also ist $A = g$. Nun erhält man aus dem Reziprozitätsgesetz unmittelbar, daß das Produkt sämtlicher Charaktere gleich 1 ist [7]). Demnach ist die Anzahl der Geschlechter für $D \equiv 1 \pmod 4$ höchstens gleich $2^{\nu-1}$, für andere D höchstens gleich 2^{ν}. Wir erhalten also einen Widerspruch zu II.

Satz 5 [8]). *Ist D eine quadratfreie natürliche Zahl, so ist eine und nur eine der Gleichungen*

$$D_1 u^2 - D_2 v^2 = \varepsilon, \quad \varepsilon = \pm 1, \pm 2, \quad D_1 D_2 = D, \quad D_1 < D_2, \tag{2}$$

wo $\varepsilon = -1$ für $D_1 = 1$, in natürlichen Zahlen u, v lösbar.

Beweis. I. Zunächst bemerken wir, daß mindestens eine der Gleichungen (2) lösbar ist. Um dies einzusehen, betrachten wir die kleinsten natürlichen Zahlen t, w, für die $t^2 - Dw^2 = 1$ ist. Man erhält dann, daß für gewisse ganze rationale Zahlen α, β, D_1, D_2, v_1, v_2

$$t + 1 = 2^{\alpha} D_1 v_1^2, \quad t - 1 = 2^{\beta} D_2 v_2^2, \quad D = D_1 D_2, \quad 0 \leqq \alpha + \beta \leqq 2.$$

Also ist $2 = 2^{\alpha} D_1 v_1^2 - 2^{\beta} D_2 v_2^2$ eine Gleichung vom Typus (2).

II. Es sei $D_1 x^2 - D_2 y^2$ die Form aus I, für die $D_1 x^2 - D_2 y^2 = \varepsilon$ lösbar ist. Demnach erhält man sämtliche Lösungen der Pellschen Gleichung $x^2 - Dy^2 = 1$ aus $\left(\frac{\sqrt{D_1}x + \sqrt{D_2}y}{\sqrt{|\varepsilon|}}\right)^{2k}$, wo k eine ganze rationale Zahl bezeichnet. Wäre $d_1 x^2 - d_2 y^2 = \varepsilon_1$, $\varepsilon_1 = \pm 1, \pm 2$ eine andere Lösung von (2), so würde für eine gewisse ganze rationale Zahl n

$$\frac{\sqrt{d_1}x \pm \sqrt{d_2}y}{\sqrt{|\varepsilon_1|}} = \pm \left(\frac{\sqrt{D_1}x + \sqrt{D_2}y}{\sqrt{|\varepsilon|}}\right)^{n}$$

sein, denn $\left(\frac{\sqrt{d_1}x + \sqrt{d_2}y}{\sqrt{|\varepsilon_1|}}\right)^{2}$ ergibt wieder eine Lösung der Pellschen Gleichung. Mithin hat (2) höchstens eine Lösung.

---

[7]) Vgl. z. B. Cahen, a. a. O.[4]), S. 399—403; nach Hilbert ist dies der eigentliche Sinn des Reziprozitätsgesetzes.

[8]) K. Petr, Über die Pellsche Gleichung, Časopis **56** (1927), S. 57—66.

Eingegangen 2. Juni 1936.