Sonder-Vorlesung:

"Der 3-Quadratesatz mit Gauß"

$\boxed{n \in \mathbb{N}}$ gegeben. O.E. $n \not\equiv 0 \bmod 4$.
Denn: $4m = x_1^2+x_2^2+x_3^2$ in $\mathbb{Z}$, $\Rightarrow$ alle $x_i \in 2\mathbb{Z}$, $\Rightarrow m = y_1^2+y_2^2+y_3^2$ in $\mathbb{Z}$
(und umgekehrt)

Satz (Legendre 1798, Gauß 1801): Sei $n \equiv 1, 2, 3, 5$, oder $6 \bmod 8$.[1] Dann

(1) $$n = x_1^2 + x_2^2 + x_3^2 \text{ in } \mathbb{Z}$$ [2]

Diese Behauptung liegt anscheinend ziemlich tief. Nach heutigem Stand ist sie aus einem allgemeinen Prinzip der Algebraischen Zahlentheorie, dem sogenannten Lokal-Global-Prinzip von Hasse, herleitbar. Was möglichst direkte Beweise angeht, so sei ein im Netz kursierender Beweis von O. Forster genannt sowie das bekannte Buch von J.P. Serre. Die berufen sich allerdings auf den bekannten Primzahlsatz von Dirichlet, wonach in jeder Restklasse a modulo m für bel. m unendlich viele Primzahlen liegen, falls a teilerfremd zu m ist. Eine einfache u. einleuchtende Aussage, deren Beweis aber nicht weniger Finesse verlangt wie der des 3-Quadratesatzes. – Im übrigen wird bei Forster u. Serre erst nur eine "Vorstufe" von (1) bewiesen, nämlich

(2) $$n = r_1^2 + r_2^2 + r_3^2 \text{ in } \mathbb{Q}$$

Die verbleibende Begründung von (2) $\Longrightarrow$ (1) ist zwar nicht besonders schwer, liegt aber auch nicht auf der Hand (und ist sozusagen ein "Glücksfall", denn bei mehr als 3 Quadraten würde sie versagen.)
Einen direkten Beweis von (1) – ohne die Vorstufe (2) – gab Dirichlet 1850, natürlich auch unter Einsatz seines PZ-Satzes. Dieser schöne Beweis ist anscheinend wenig verbreitet. Widergespiegelt fand ich ihn in einer Vorlesungsnachschrift von K. Heliposrky. Dirichlet merkt an, daß die viel komplizierteren Betrachtungen von Gauß aber nötig seien, wenn auch die Anzahlen der Darstellungen (1) zu erfassen. – Im übrigen kannten Gauß und

[1] $n \equiv 7 \bmod 8$ scheidet von vornherein aus, denn 7 ist nicht Summe dreier Quadrate in $\mathbb{Z}$, ebensowenig wie 7 modulo 8.

[2] Diese Aussage ist eigentlich noch nicht der vollständige Inhalt des 3-Quadratesatzes, vgl. (1^) weiter unten.

Dirichlet einen Zusatz von (1), auf den schon Legendre besonderen Wert gelegt hatte (der aber in der modernen Literatur, namentlich bei Serre unerörtert bleibt), nämlich daß n auch eine primitive Darstellung als Summe dreier Quadrate in $\mathbb{Z}$ besitzt, d.h. daß

$$(1') \qquad n = x_1^2 + x_2^2 + x_3^2 \text{ in } \mathbb{Z} \text{ mit } \operatorname{ggT}(x_1, x_2, x_3) = 1$$

gilt. Dies war von Legendre mit Recht hervorgehoben, denn während etwa 45 i.w. nur eine einzige Darstellung als Summe zweier Quadrate besitzt, nämlich $45 = 6^2 + 3^2$, hat 45 neben $45 = 6^2 + 3^2 + 0^2$ noch die primitive Darstellung $45 = 5^2 + 4^2 + 2^2$ als Summe dreier Quadrate.[1) 2)]

Legendre, der den 3-Quadratesatz zuerst klar und deutlich ausgesprochen hat, widmet ihm viele Seiten seines Buches. Ich habe mich da nicht durchgekämpft, kann also nicht mit Bestimmtheit sagen, ob Legendre seinen Satz wirklich bewiesen hat. Eher nicht, so glaubte ich, auch wegen diesbezüglicher Anmerkungen von Gauß. Diese beziehen sich aber vielleicht auf die 1. Auflage von Legendres Buch, nicht auf die zweite. —

In Bezug auf den 3-Quadratesatz ist Dirichlets PZ-Satz eigentlich ein sachfremdes Element, noch dazu dessen Beweis ja ausgefeilte Methoden der Analysis erfordert. Wie dem auch sei, jedenfalls ist die Neugier angebracht, wie's Gauß denn nun

---

1) Für die exakte Darstellungsanzahl gilt also $r_3(45) = 24 + 48 = 72$. Zuerst schien mir das nicht in Einklang zu stehen mit der Anzahl 48, die ich Gauß entnahm; bis ich merkte, daß Gauß nur die Anzahl $R_3(n)$ der primitiven Darstellungen zählt, für die in der Tat $R_3(45) = 48$ gilt.

2) Ob man nach Beweis von (1) die zusätzliche Forderung $\operatorname{ggT}(x_1, x_2, x_3) = 1$ eventuell nachträglich noch gesondert zeigen kann, weiß ich nicht. Wenn nicht, würden auch die tiefgründigen Klassenzahlrelationen von Kronecker, die sich in Smith, Collected Math. Papers, Vol. I, S. 323 f. finden, nur die $r_3(n)$ ergeben, nicht direkt die Gaußschen $R_3(n)$, und insb. nicht $R_3(n) \neq 0$ für $n \equiv 1, 2, 3, 5, 6 \bmod 8$.

gemacht hatte (ohne Dirichlets PZ-Satz, dessen Beweis seinerzeit noch völlig in den Sternen stand, obwohl Legendre seine Aussage bereits in sein Buch aufgenommen hatte [1]).
Ich nahm also die "disquisitiones" zur Hand [2] (deren Lektüre ja jedem Zahlentheoretiker immer angeraten wird).
Ich erlebte ein Fiasko: Wo ich auch ansetzte, biß ich auf Granit. Ich wich also erst mal aus und suchte Beistand anderswo. Viel Glück hatte ich damit nicht. Abgesehen natürlich von dem 150 Jahre alten Band der Vorlesungen Dirichlets mit den wertvollen Zusätzen Dedekinds. Und ich versuchte zu mobilisieren, was ich selbst wußte. Zum Beispiel machte ich mir klar, daß die Anwendung des Lokal-Global-Prinzips auf unser Problem lediglich darin bestand, sicherzustellen, daß die quadratische Form $X_1^2+X_2^2+X_3^2$ isotrop über dem quadratischen Zahlkörper $K=\mathbb{Q}(\sqrt{-n})$ ist. Ich will lieber nur ausführen:

Bemerkung: Ist $X_1^2+X_2^2+X_3^2$ isotrop über $\mathbb{Q}(\sqrt{-n})$, so gilt (2).

Bew. Nach Vor. ist $\sum_{i=1}^{3}(x_i+y_i\sqrt{-n})^2=0$ mit $x_i, y_i \in \mathbb{Q}$, nicht alle 0.
Dies ist äquivalent mit $\sum x_i^2 - n\sum y_i^2 = 0$, $\sum x_i y_i = 0$ und $\sum y_i^2 \neq 0$.
Es folgt $\left(\sum y_i^2\right)^2 = \sum_1^3 x_i^2 \sum_1^3 y_i^2 \overset{!}{=} \sum_1^3 z_i^2$ (und damit die Beh.)
Wo kommen die $z_i \in \mathbb{Q}$ her? Man betrachte die "reinen Quaternionen" $x = x_1 i + x_2 j + x_3 k$, $y = y_1 i + y_2 j + y_3 k$. Da sie zueinander orthogonal sind, ist ihr Produkt xy wieder ein reines Quaternion $z_1 i + z_2 j + z_3 k$. Übergang zu den Normen liefert die Behauptung. □

Damit leuchtete mir auf einmal bei Gauß etwas ein, was mir zuerst sehr befremdlich erschienen war. Nämlich daß Gauß die Darstellung binärer quadr. Formen durch ternäre

[1] Dirichlet bewies den Satz 1837 [2] in der deutschen Übersetzung von H. Maser

quadr. Formen betrachtet. Alle Koeffizienten stets als ganzzahlig vorausgesetzt. Sei $F = \begin{pmatrix} a_1 & b_1 & b_2 \\ b_1 & a_2 & b_3 \\ b_2 & b_3 & a_3 \end{pmatrix}$ eine symmetrische 3×3-Matrix über $\mathbb{Z}$, und mit F werde auch die von ihr vermittelte quadr. Form bezeichnet: $F(X_1,X_2,X_3) = a_1X_1^2 + a_2X_2^2 + a_3X_3^2 + 2b_1X_1X_2 + \ldots$. Entsprechend vermittelt eine symmetrische 2×2-Matrix $\varphi = \begin{pmatrix} a & b \\ b & c \end{pmatrix}$ die binäre quadr. Form

$$\varphi(X,Y) = aX^2 + 2bXY + cY^2 \tag{3}$$

Gauß sagt, φ werde durch F dargestellt, wenn es ganze $x_1, y_1, x_2, y_2, x_3, y_3$ gibt mit

$$F(x_1X + y_1Y, x_2X + y_2Y, x_3X + y_3Y) = \varphi(X,Y) \tag{4}$$

Was folgt, verlangt Gauß durch leichte Rechnung zu bestätigen. Es geht auch (fast) ohne Rechnung und sei deshalb als Übungsaufgabe gestellt:

Üb. 1: Sei $\tilde{F}$ die komplementäre Matrix zu F [1]. Aus (4) folgt dann $\tilde{F}(x_2y_3 - x_3y_2, x_3y_1 - x_1y_3, x_1y_2 - x_2y_1) = -D$ mit $\boxed{D = b^2 - ac}$ als "Diskriminante von φ". [2]

Bemerkung: Was ich hier Diskriminante von φ nenne, heißt bei Gauß die "Determinante" von φ, obwohl doch $\begin{pmatrix} a & b \\ b & c \end{pmatrix}$ die Determinante $-D$ hat. Auch würde man heute unter einer (ganzzahligen) binären qu. Form jedes Polynom der Gestalt

$$aX^2 + BXY + cY^2 \qquad (\text{mit } a, B, c \in \mathbb{Z})$$

verstehen, und $\hat{D} = B^2 - 4ac$ ihre Diskriminante nennen. Es läßt sich darüber wenigstens sagen: Nennen wir die Formen der Gestalt (3) "klassisch", so gilt:

---

1) Sie erfüllt $F\tilde{F} = \tilde{F}F = \det(F)E$. 2) (4) besagt, daß die Matrix $\begin{pmatrix} a & b \\ b & c \end{pmatrix}$ Produkt dreier Matrizen, darunter F, ist. Übergang zu den Matrizen der 2×2-Unterdeterminanten ist multiplikativ und liefert unter Berücksichtigung von Vorzeichen die Behauptung.

klassische binäre qu. Formen zu D $\hat{=}$ binäre qu. Formen zu $\hat{D} = 4D$

Gauß betrachtet also sozusagen "nur die Hälfte aller binären qu. Formen"; für die Anwendung auf den 3-Quadratesatz ist das jedenfalls ausreichend. Im Folgenden bleiben wir bei den klassischen Formen von Gauß und halten uns überhaupt an seine Notation; nur seine Bezeichnung "Determinante von φ" ersetzen wir durch <u>Diskriminante von φ</u>.

<u>Def. 1</u>: Die Form φ in (3) bezeichnen wir mit $\varphi = [a,b,c]$. Geht $\psi = \varphi \circ S$ durch eine Substitution S aus $SL_2(\mathbb{Z})$ hervor, so nennen wir ψ <u>äquivalent</u> zu φ und schreiben $\psi \simeq \varphi$. Die so definierten Äquivalenzklassen heißen kurz <u>Klassen</u>. Alle Formen einer Klasse haben dieselbe Diskriminante und stellen dieselben Zahlen dar. Für die Klasse von $\varphi = [a,b,c]$ werde ich oft keine gesonderte Bezeichnung verwenden, sondern sie ebenfalls mit $\varphi = [a,b,c]$ bezeichnen. Gauß zeigt, daß es nur <u>endlich viele Klassen</u> mit gegebener Diskriminante D gibt; hier und im Folgenden werde vorausgesetzt, daß D <u>kein Quadrat in $\mathbb{Z}$</u> ist, also insb. $D \neq 0$.

<u>Def. 2</u>: $\varphi = [a,b,c]$ heißt <u>primitiv</u>, wenn $ggT(a,b,c) = 1$. Daneben ist natürlich

$$\sigma := ggT(a, 2b, c)$$

zu betrachten. Sei φ <u>primitiv</u>. Ist sogar $\sigma = 1$, so heißt φ <u>eigentlich primitiv</u>, ich sage kurz <u>1-primitiv</u>; ist $\sigma = 2$, so heißt φ <u>uneigentlich primitiv</u>, ich sage kurz <u>2-primitiv</u>. Ist φ 2-primitiv, so sind <u>a und c gerade</u>, aber <u>b ungerade</u>; für $D = b^2 - ac$ gilt daher notwendig $\boxed{D \equiv 1 \bmod 4}$.[1] Die Begriffe 1-primitiv und 2-primitiv sind unter Äquivalenz invariant. <u>Für gegebenes</u> D bezeichnen wir mit

(5) $\mathcal{C}$ die Klassen der 1-primitiven Formen der Diskriminante D
$\mathcal{C}_0$ — " — 2-primitiven — " —

[1] Nur im Falle $D \equiv 1 \bmod 4$ also sind 2-primitive Formen möglich. Im Lichte heutiger Notation (siehe oben) wirken die 2-primitiven Formen etwas unnatürlich. Beim Gaußschen Beweis des 3-Quadratesatzes scheinen sie aber <u>unentbehrlich</u> zu sein.

Leicht zu zeigen, aber später wichtig, ist folgender Sachverhalt:

ÜG2: Sei $N \in \mathbb{N}$ beliebig[1], und sei φ primitiv mit Diskriminante D. Ist φ 1-primitiv, so nimmt φ unendlich viele Werte $a=\varphi(x,y)$ an, die zu N teilerfremd sind; insbesondere gilt

(6) $$\varphi \simeq [a,b,c] \quad \text{mit} \quad ggT(a,2D)=1$$

Ist φ 2-primitiv, so nimmt φ unendlich viele Werte $2a_0=\varphi(x,y)$ an, für die a_0 teilerfremd zu N ist; insb. gilt

(7) $$\varphi \simeq [2a_0,b,c] \quad \text{mit} \quad ggT(a_0,2D)=1$$

Im Folgenden denken wir uns eine 1- bzw. 2-primitive Form φ stets wie in (6) bzw. (7) gegeben.

Alles, was ich bisher ausgeführt habe – mit vielleicht zu viel Worten – hatte mehr einführenden Charakter. Relativ 'zahm' war es auch in mathematischer Hinsicht, ausgenommen vielleicht die behauptete Endlichkeit der Mengen $\mathcal{C}$ (und $\mathcal{C}_0$) in (5). Diese ist aber auch eher einleuchtend als überraschend und jedenfalls nicht tiefgründig im Falle $D<0$, auf den es im Zusammenhang mit dem 3-Quadratesatz nur ankommt. – Was nun den Beweis des 3-Quadratesatzes angeht, so beweist ihn Gauß erst am Ende des längsten Kapitels der 'disquisitiones', als Anwendung einer ausgebauten Methodik, namentlich der von ihm erfundenen "Komposition binärer qu. Formen" sowie seiner "Geschlechtertheorie". Der Punkt, auf den es beim Beweis des 3-Quadratesatzes ankommt, ist folgende

Existenzaussage: Zu $D=-n$ mit $n=1,2,3,5$ oder $6 \bmod 8$ gibt es eine primitive[2] binäre Form $\varphi=(a,b,c)$ mit folgenden Eigenschaften: (i) $a<0$ (d.h. φ ist negativ definit) (ii) a ist QR mod p für jedes $p \mid D$.[3]

---

1) Im Beweis betrachte man zunächst den Fall $N=p$ einer Primzahl. 2) φ ist 1-primitiv bis auf den Fall $n\equiv 3 \bmod 8$, d.h. $D\equiv 5 \bmod 8$, vgl. w.u.

3) Vereinbarungsgemäß ist a prim zur Diskriminante D von φ.

Beweis des 3-Quadratsatzes (auf die fraglich verbleibende Existenzaussage):

Sei also $\varphi = (a,b,c)$ wie angegeben. Wegen $D \not\equiv 0 \bmod 4$ gilt ~~nach~~ (ii):
a ist QR mod D, d.h. es gibt ein $B \in \mathbb{Z}$ mit

$$\boxed{B^2 \equiv a \bmod D}$$

Wir haben ein B' mit $B'a \equiv -Bb \bmod D$; es folgt $\boxed{BB' \equiv -b \bmod D}$,
und damit weiter $aB'^2 \equiv b^2 \bmod D$, also auch $aB'^2 \equiv b^2 + (ac - b^2) \bmod D$,
mithin $\boxed{B'^2 \equiv c \bmod D}$. Setzt man $\boxed{A'' := D}$, so hat man also wohlbestimmte ganze A', B'', A mit

(α) $B^2 - A'A'' = a$ $\quad(\beta)$ $BB' - B''A'' = -b$ $\quad(\gamma)$ $B'^2 - AA'' = c$

ÜA 3: $\exists\ G = \begin{pmatrix} a & b & b_2 \\ b & c & b_3 \\ b_2 & b_3 & a_3 \end{pmatrix} \in M_3(\mathbb{Z})$ mit $\boxed{\det(G) = -1}$ [und a, b, c wie oben],

so daß die komplementäre Matrix $\tilde{G}$ von G die Gleichung

$$(8) \qquad \tilde{G} = -\begin{pmatrix} A & B'' & B' \\ B'' & A' & B \\ B' & B & A'' \end{pmatrix}$$

erfüllt, mit A, A', A'', B, B', B'' als den in $(\alpha), (\beta), (\gamma)$ genannten Zahlen. □

Nach Erledigung von ÜA 3[1] verläuft die Argumentation wie folgt:
Sei also G wie behauptet. Wegen $a < 0$, $\begin{vmatrix} a & b \\ b & c \end{vmatrix} = -D > 0$, $\det(G) < 0$ ist G negativ definit, und hat wie gesagt die Determinante -1.

Wie Gauß weiß (und auch relativ leicht zu zeigen ist, vgl. Art. 277 der Disquisitiones) gibt es bis auf Äquivalenz nur eine solche ternäre Form, nämlich $F := -(X^2 + Y^2 + Z^2)$. Zu dieser ist G also äquivalent, d.h. es existiert eine Matrix

---

1) Zur Lösung von ÜA 3 macht Gauß nur Andeutungen. Hier habe ich mir nur durch "Rechnerei" zu helfen gewußt, siehe w. u.

(9) $\quad S = \begin{pmatrix} x_1 & x_2 & x_3 \\ y_1 & y_2 & y_3 \\ z_1 & z_2 & z_3 \end{pmatrix} \in SL_3(\mathbb{Z})$ mit

$F(x_1X+y_1Y+z_1Z,\, x_2X+y_2Y+z_2Z,\, x_3X+y_3Y+z_3Z) = G = aX^2+cY^2+a_3Z^2+2bXY+2b_2XZ+2b_3YZ.$

Setzt man hier $Z=0$, so erhält man

$$F(x_1X+y_1Y,\, x_2X+y_2Y,\, x_3X+y_3Y) = aX^2+cY^2+2bXY \overset{!}{=} \varphi\,,$$

d.h. die obige binäre Form φ wird durch die ternäre Form $F = -(X^2+Y^2+Z^2)$ dargestellt. Nach ÜB 1 stellt dann die komplementäre Form $\tilde{F}$ die Zahl $-D$ dar, genauer:

$$\tilde{F}(x_2y_3-x_3y_2,\, x_3y_1-x_1y_3,\, x_1y_2-x_2y_1) = -D = n$$

Nun ist aber $\tilde{F}$ einfach die Form $\tilde{F} = X^2+Y^2+Z^2$, also gilt

(10) $\qquad n = x^2+y^2+z^2$

mit $x = x_2y_3-x_3y_2$, $y = x_3y_1-x_1y_3$, $z = x_1y_2-x_2y_1$. Und wegen $\det(S) = z_1x + z_2y + z_3z = 1$ gilt auch

(11) $\qquad \mathrm{ggT}(x,y,z) = 1.$ $\qquad\square$

<u>Zur (technischen) Lösung von ÜB 3:</u> <u>1)</u> Die gesuchten b_2, b_3 und a_3 sind bereits durch drei der sechs in (8) geforderten Gleichungen bestimmt, nämlich die Gleichungen

(12) $ab_3 - bb_2 = B, \quad -bb_3 + cb_2 = B', \quad b_2^2 - aa_3 = A'$

Dabei ergeben sich b_2, b_3 aus den beiden ersten mittels der <u>Cramerschen Regel</u> und a_3 einfach durch $a_3 = \frac{b_2^2 - A'}{a}$. Allerdings sind b_2, b_3, a_3 zunächst nur <u>rationale Zahlen</u>.

<u>2)</u> Die an G gestellte Determinantenbedingung $\det(G) = -1$ besagt

(13) $\quad b_2(bb_3 - cb_2) - b_3(ab_3 - bb_2) + a_3(-A'') = -\underline{1}$

und ist (nach Multipl. mit a) äquivalent zu

$ab_2(bb_3-cb_2)-ab_3(ab_3-bb_2)+(A'-b_2^2)A''+a=0$, also wegen obiger Gleichung (α), d.h. $A'A''=B^2-a$ zu

$$2abb_2b_3-acb_2^2-a^2b_3^2-b_2^2A''+B^2=0,$$ und damit wegen der 1. Gleichung in (12) zu

$$2abb_2b_3-acb_2^2-a^2b_3^2-b_2^2A''+a^2b_3^2-2abb_2b_3+b^2b_3^2=0$$

Auf der linken Seite hebt sich wegen $A''=b^2-ac$ in der Tat alles weg.

3) Um für das erhaltene G mit $\det(G)=-1$ auch die Relation (8) zu zeigen, bleibt nach (12) noch, folgende 3 Gleichungen zu verifizieren:

(14) $\quad b_3^2-ca_3=A, \quad a_3b-b_3b_2=B'', \quad b^2-ac=A''$

wobei die dritte schon klar ist, denn es war $A''=D=b^2-ac$. — Die erste Gleichung in (14) ist äquivalent zu $b_3^2A''-ca_3A''=AA''$, wegen obiger Gleichung (γ) also zu

(*) $\quad b_3^2A''-ca_3A''=B'^2-c$

Nach (13) ist $a_3A''=1+b_2(bb_3-cb_2)-b_3(ab_3-bb_2)=$
$1-cb_2^2-ab_3^2+2bb_2b_3$, so daß (*) äquivalent ist zu

$$B'^2=b_3^2A''+c(cb_2^2+ab_3^2-2bb_2b_3);$$ wegen $B'=cb_2-bb_3$ also zu

$$c^2b_2^2-2bcb_2b_3+b^2b_3^2=b_3^2A''+c^2b_2^2-2bcb_2b_3+acb_3^2$$

Hier hebt sich – wieder wegen $A''=b^2-ac$ – in der Tat alles weg. —
Jetzt ist noch $a_3b-b_3b_2=B''$ zu zeigen. Dies ist wegen obiger Gleichung (β), also $A''B''=b+BB'$ äquivalent zu
$BB'+b=a_3A''b-b_2b_3A''$, mit Blick auf (12) also zu

$$(ab_3-b_2b)(cb_2-b_3b)+b=a_3A''b-b_2b_3A'',$$ d.h. zu

(**) $\quad acb_2b_3-abb_3^2-bcb_2^2+b_2b_3b^2+b(1-a_3A'')=-b_2b_3(b^2-ac)$

Nach (13) ist $1-a_3A''=b_2(cb_2-bb_3)+b_3(ab_3-bb_2)$. Setzt man das in (**) ein, so hebt sich wieder alles weg.

4) Wir bezeichnen mit H die rechte Seite von (8). Wir haben (8) schon bewiesen, d.h. unser G erfüllt (neben $\det(G) = -1$) auch

$$G^\sim = H$$

Daraus folgt $\tilde{H} = \tilde{\tilde{G}} = \det(G)G = -G$. Da H nur ganze Koeffizienten hat, gilt dies auch für $\tilde{H}$, und damit auch für G. Damit liegen die in 1) konstruierten rationalen Zahlen b_2, b_3, a_3 wirklich alle in $\mathbb{Z}$. $\square$

Es sei nun versucht, wenigstens eine gewisse Vorstellung von der Gaußschen Theorie der binären qu. Formen zu vermitteln, und davon, wie man damit die obige Existenzaussage (vgl. S. VI) erhält, auf die wir uns beim Beweis des 3-Quadratesatzes gestützt haben.

1. Zur "Composition" binärer qu. Formen

Von Gauß erfunden, aber in den disquisitiones sehr schwierig nachzuvollziehen, heutzutage gehört dazu schon fast indische Leidensfähigkeit wie z.B. des Fields-Medaillisten Bhargava, hoch gelobt eben auch wegen kreativer Neuinterpretation der Gaußschen Composition binärer qu. Formen (mit Erschließungsmöglichkeit analoger "höherer Kompositionsgesetze"). Habe mir Bhargavas erste Arbeit in dieser Richtung mal angesehen. Sein Ansatz ist in der Tat bestechend; aber wer erwartet, er würde nun mit noch ein paar Worten einen Beweis seines Theorem 1 machen, wird enttäuscht. Er verweist auf einen späteren Abschnitt, und da geht es auch ziemlich technisch zu. Außerdem beschränkt sich Bhargava bei der Komposition (Multiplikation) binärer qu. Formen allein auf die Menge $\mathcal{C}$ der 1-primitiven Formen. Aber das reicht für unsere Zwecke nicht aus. Was wir mindestens brauchen ist Komposition einer beliebigen

1-primitiven Form φ mit einer <u>beliebigen primitiven</u> Form φ', sei φ' nun 1- oder 2-primitiv. Dabei halten wir uns an Dirichlet-Dedekind. Man denke sich $\varphi \simeq [a,b,c]$ und $\varphi' = [a',b',c']$ zunächst gemäß <u>ÜA2</u> gegeben und außerdem so, daß $\boxed{ggT(a,a',b+b')=1}$ gilt.[3] Wie Dirichlet-Dedekind nun (unschwer) zeigen, gibt es ganze B und C mit

(15) $\varphi \simeq [a, B, a'C]$ und $\varphi' \simeq [a', B, aC]$

mit <u>gleichen</u> mittleren Koeffizienten B und so, daß die dritten Koeffizienten der jeweils anderen Form durch Multiplikation mit demselben Faktor C hervorgehen.) Man definiert dann die Komposition (das <u>Produkt</u>) $\varphi\cdot\varphi'$ durch

(16) $$\varphi\cdot\varphi' = [aa', B, C]$$

Damit gilt nun nach Dirichlet-Dedekind:

(17) $\mathcal{C}$ ist eine (abelsche) <u>Gruppe</u>[1]

(18) Die Gruppe $\mathcal{C}$ operiert <u>transitiv</u> auf $\mathcal{C}_0$ [2] [3]

Da die Gruppe $\mathcal{C}$ <u>endlich</u> ist, gilt nach (18) für die Elementanzahlen

(19) $\#\mathcal{C} = r\cdot\#\mathcal{C}_0$ mit einem $r \in \mathbb{N}$

---

1) Die Klasse der Form $[1,0,D] = X^2 - DY^2$ heißt die <u>Hauptklasse</u> von $\mathcal{C}$. Wie leicht zu sehen, gilt: Stellt eine binäre Form (zu D) die Zahl 1 dar, so gilt $\varphi \simeq [1,0,D]$. Für bel. $\varphi' = [a',b',c']$ in $\mathcal{C}$ oder $\mathcal{C}_0$ folgt $[1,0,D]\cdot\varphi' = [1,b',*]\cdot[a',b',*] = [a',b',*] \simeq \varphi'$. Also ist die Hauptklasse das <u>Einselement</u> der Gruppe $\mathcal{C}$. Das <u>Inverse</u> von $\varphi \simeq [a,b,c]$ aus $\mathcal{C}$ ist $\varphi^{-1} := [c,b,a] \simeq [a,-b,c]$. Denn $[a,b,c]\cdot[c,b,a] \simeq [ac,b,1] \simeq [1,0,D]$.

2) Solche Formulierung findet sich natürlich nicht bei <u>Gauß</u>, und auch nicht bei <u>Dedekind</u>, und so ist dort nicht auf Anhieb zu erkennen, um was es an betreffender Stelle eigentlich geht. Gleiches gilt für die aus heutiger Sicht selbstverständliche Folgerung (19). – [3] Nochmals sei auch daran erinnert: Von $\mathcal{C}_0$ kann die Rede nur sein, wenn $D \equiv 1 \bmod 4$ ist.

3) Sogar $ggT(a,a') = 1$. Aber im Folgenden ist es praktisch, nur $ggT(a,a',b+b') = 1$ vorauszusetzen.

Bemerkung: Sei $D \equiv 1 \bmod 4$, und sei $[2, 1, \frac{1-D}{2}]$ die "einfachste" 2-primitive Form zu D. Für ein beliebiges $f \in \mathcal{C}$ ist dann $\varphi := f \cdot [2, 1, \frac{1-D}{2}]$ in $\mathcal{C}_0$. Umgekehrt hat jedes $\varphi \in \mathcal{C}_0$ nach (18) die Gestalt

(20) $$\varphi = f \cdot [2, 1, \tfrac{1-D}{2}] \text{ mit einem } f \in \mathcal{C}.$$

– Im übrigen sind für den Faktor r in (19) nur die Werte $r=1$ oder $r=3$ möglich, wie Gauß zeigte (man liest das am besten bei Dirichlet-Dedekind nach). Darüberhinaus beweist Gauß:

(21) Im Falle $D<0$ ist $r=3$ mit Ausnahme von $D=-3$.

2. Zu den "Geschlechtern" binärer qu. Formen

Was Gauß hier macht – wenn auch in etwas anderer Notation – ist etwa das Folgende: Er betrachtet eine wohlbestimmte Familie

(21) $$\chi_1, \chi_2, \ldots, \chi_\lambda$$

von sogenannten "Spezialcharakteren", als Funktionen auf $\mathcal{C}$ bzw. $\mathcal{C}_0$. Hierzu gehören erstens die Legendre-Symbole $\chi_p = \left(\frac{\cdot}{p}\right)$ für die $p \mid D$, zweitens gewisse der (drei nichttrivialen) Charaktere $\chi_2 \bmod 8$ und drittens[1] – dies aber nur im Falle $D<0$ – $\chi_\infty(\varphi) = \operatorname{sgn}(\varphi) = \operatorname{sgn}(a)$. [mit sgn als der Signatur von φ bzw. dem Vorzeichen von a]

Für $\varphi = [a,b,c] \in \mathcal{C}$ bzw. $\varphi = [2a_0, b, c] \in \mathcal{C}_0$ wie in Üb2 sei dabei

(22) $$\chi_p(\varphi) = \left(\frac{a}{p}\right) \qquad \text{bzw.} \quad \chi_p(\varphi) = \left(\frac{a_0}{p}\right)$$

Dies ist wohldefiniert, denn konkurriert $a' = \varphi(x,y)$ mit a, so gilt $aa' = a\varphi(x,y) = a(ax^2 + 2bxy + cy^2) = (ax+by)^2 - Dy^2$, also ist aa' QR mod p für

---

[1] nicht so bei Gauß. Doch die "Stelle $p=\infty$" von vornherein mit einzubeziehen, ist unerläßlich. Wir nehmen dafür in Kauf, daß $\mathcal{C}$ im Falle $D<0$ nicht die gewohnte Klassengruppe nur der positiv definiten binären Formen bezeichnet, sondern auch die negativ definiten einschließt.

jedes $p|D$. ⌈Analog im Falle $\varphi\in\mathcal{C}_0$⌋. – Entsprechend zeigt man auch die Wohldefiniertheit etwaiger χ_2, wobei wir diese nun nochmal genauer angeben:

(23)
$D\equiv 1 \bmod 4$: kein χ_2
$D\equiv 3 \bmod 4$: $\chi_2(a)=(-1)^{\frac{a-1}{2}}$
$D\equiv 4 \bmod 4$: $\chi_2(a)=(-1)^{\frac{a-1}{2}}$
$D\equiv 2 \bmod 8$: $\chi_2(a)=(-1)^{\frac{a^2-1}{8}}$
$D\equiv 6 \bmod 8$: $\chi_2(a)=(-1)^{\frac{a-1}{2}+\frac{a^2-1}{8}}$
$D\equiv 0 \bmod 8$: sowohl $(-1)^{\frac{a-1}{2}}$ als auch $(-1)^{\frac{a^2-1}{8}}$

Mit $\boxed{\mu := \#\{p|D,\ p\neq 2\}}$ als der Anzahl der ungeraden Primteiler von D gilt demnach für die Anzahl λ aller in (21) genannten Spezialcharaktere, wenn wir uns mal auf den Fall $\boxed{D<0}$ beschränken:

(24)
$\lambda=\mu+1$ für $D\equiv 1,5 \bmod 8$; $\lambda=\mu+3$ für $D\equiv 0 \bmod 8$;
$\lambda=\mu+2$ für $D\equiv 2,3,4,6,7 \bmod 8$;

Mit Blick auf die Definition der Komposition binärer qu. Formen $\varphi\in\mathcal{C}$ und $\varphi'\in\mathcal{C}$ bzw. $\mathcal{C}_0$ gilt

(25) $\chi_i(\varphi\varphi') = \chi_i(\varphi)\chi_i(\varphi')$ für jedes $1\le i\le\lambda$ ⌈vgl. (16)⌋

Auf $\mathcal{C}$ vermitteln die χ_i also (quadratische) Charaktere χ_i, und der "Totalcharakter" $\chi=(\chi_1,\dots,\chi_\lambda)$ vermittelt einen Homomorphismus

(26) $\chi:\ \mathcal{C}\longrightarrow\{+1,-1\}^\lambda$

Definition: $\varphi,\psi\in\mathcal{C}$ gehören zum selben Geschlecht, wenn $\chi(\varphi)=\chi(\psi)$ gilt, d.h. $\chi_i(\varphi)=\chi_i(\psi)$ für jedes $1\le i\le\lambda$. ⌈Ebenso läßt sich auch $\mathcal{C}_0$ in Geschlechter einteilen.⌋

1) Meine ursprüngliche Mutmaßung, worauf die Gaußsche Einteilung in Geschlechter eigentlich hinausläuft, fand ich im Springer-Text von Zagier bestärkt, wo es S. 108 mit historischem Bezug auf Gauß heißt: "Man sagt, daß zwei Formen ⌈gleicher Diskriminante⌋, die rational äquivalent sind ⌈d.h. über $\mathbb{Q}$⌋, zum selben Geschlecht gehören." Von rationaler Äquivalenz ist freilich in den 'Disquisitiones' nirgends die Rede. Doch bei Betrachtung gewisser Beispiele wie z.B. $D=-75$ stellte ich fest, daß die Anzahl obiger 'rationaler Geschlechter' kleiner ausfiel als die Geschlechterzahl bei Gauß. Was bei Zagier steht, kann so also nicht stimmen. Richtig ist es nur für solche D, die als Diskriminanten quadratischer Zahlkörper auftreten.

Die Geschlechter von $\mathcal{C}$ lassen sich demnach als Elemente der Gruppe $\mathfrak{G} = \mathcal{C}/\mathrm{Ker}\,\mathcal{X}$ ansehen. Das Einselement von $\mathfrak{G}$, also $\mathrm{Ker}\,\mathcal{X}$ heißt das Hauptgeschlecht; es besteht aus allen Klassen in $\mathcal{C}$, die im selben Geschlecht wie die Hauptklasse $[1,0,D]$ liegen. Mit Blick auf (26) können wir die Geschlechtergruppe $\mathfrak{G}$ als Untergruppe der Gruppe $\{1,-1\}^\lambda$ ansehen. Wie Gauß zeigt, gilt

(27) Anzahl der Geschlechter $= \#\mathfrak{G} = 2^{\lambda-1}$,

d.h. $\mathfrak{G}$ ist eine Untergruppe vom Index 2 in der Gruppe $\{1,-1\}^\lambda$. Oder wie Gauß-in-etwa-sagt: genau der Hälfte aller denkbaren Charakterenwerte entsprechen „wirklich existierende Geschlechter". Und „diese Hälfte" wird von Gauß auch genauer beschrieben. Wir folgen darin aber Dirichlet (mit kleiner Abweichung): Für jedes $\varphi=[a,b,c]\in\mathcal{C}$ mit a prim zu 2D betrachte man das Jacobi-Symbol $\left(\frac{D}{a}\right)$. Wegen $D=b^2-ac$ gilt

(28) $$\left(\frac{D}{a}\right) = 1$$

Anwendung des Reziprozitätsgesetzes [vgl. S. 114] führt nun, wie leicht zu sehen, zu einer wohlbestimmten Relation

(29) $$\prod_{j\in T}\chi_j(\varphi) = 1,$$

mit Produktbildung über eine gewisse nichtleere Teilmenge $T=T(D)$ von $\{1,2,\dots,\lambda\}$. [Näheres dazu siehe w.u.] Die

---

Fortsetzung der Fußnote 1) auf S. XIII: Sind $\varphi,\psi\in\mathcal{C}$ vom selben Geschlecht (im Sinne von Gauß), so sind φ und ψ über allen $\mathbb{Q}_p$, einschließlich von $\mathbb{Q}_\infty=\mathbb{R}$, äquivalent. Das Umgekehrte gilt aber nicht generell. Zum Beispiel stimmen für die 1-primitiven Formen $\varphi=[4,1,19]$ und $\psi=[7,3,12]$ zu $D=-75$ sämtliche lokalen Hilbertsymbole überein, nicht aber die Legendresymbole χ_p für $p=5$.

$(\varepsilon_i)_{1\le i\le\lambda}$ aus $\{1,-1\}^\lambda$, die $\prod_{j\in T}\varepsilon_j = 1$ erfüllen, bilden eine Untergruppe vom Index 2, welche $X(\mathcal{C})$ nach (29) enthält. Da $X(\mathcal{C})$ wie gesagt aber ebenfalls vom Index 2 in $\{1,-1\}^\lambda$ ist, erhält man folgendes

Scholion: Genau dann gibt es ein $\varphi\in\mathcal{C}$ mit vorgegebenen $\varepsilon_i = \chi_i(\varphi)$ für alle $1\le i\le\lambda$, wenn

$$(30) \qquad \prod_{j\in T}\varepsilon_j = 1$$

gilt, mit T wie oben in (29). Gleiches gilt für $\mathcal{C}_0$ anstelle von $\mathcal{C}$.[1]

Beispiele: Im folgenden sei $D = t^2 D_0$ mit D_0 als dem quadratfreien Kern von D. Wir setzen $\boxed{D<0}$ voraus.

1) Im Falle $\boxed{D\equiv 1 \bmod 4}$ gibt es kein $\varphi = [a,b,c]\in\mathcal{C}$ mit

$$(31) \qquad a<0 \quad \text{und} \quad \left(\frac{a}{p}\right) = 1 \text{ für alle } p\mid D$$

Wenn doch, so liefert Anwendung des RZG auf (28) [da mit D auch $D_0\equiv 1 \bmod 4$ ist] $1 = \left(\frac{a}{D_0}\right)\mathrm{sgn}(a)$, und die Relation (29) lautet

$$(32) \qquad \prod_{p\mid D_0}\chi_p(a)\cdot\chi_\infty(a) = 1$$

Da nun nach (31) aber $\chi_p(a) = 1$ für alle $p\mid D$ gelten soll, muß $\chi_\infty(a) = 1$ sein, entgegen der Forderung $a<0$ in (31).

2) Im Fall $\boxed{D\equiv 1 \bmod 8}$ kann es auch kein $\varphi = [2a_0,b,c]\in\mathcal{C}_0$ geben, das – mit $a = 2a_0$ – die Bedingungen (31) erfüllt. Andernfalls läßt sich (28) durch $\left(\frac{D}{a_0}\right) = 1$ ersetzen, und daher würde (32) mit a_0 statt a gelten, definitionsgemäß also

---

[1] Letzteres folgt aus der vorigen Aussage, vgl. die Bemerkung auf S. XIII. Denn wegen (25) ist $\chi_i(f[2,1,\frac{1-D}{2}]) = \chi_i(f)$ für alle $1\le i\le\lambda$.

$$(33)\qquad \prod_{p|D_0} \chi_p(\varphi)\cdot\chi_\infty(\varphi) = 1 \qquad \ulcorner \chi_p(\varphi)=\left(\tfrac{a_0}{p}\right),\ \chi_\infty(\varphi)=\mathrm{sgn}(a_0)=\mathrm{sgn}(a)\lrcorner$$

Aus der Forderung $\left(\frac{a}{p}\right)=1$ für alle $p|D$ folgt nun $\left(\frac{a_0}{p}\right)=\left(\frac{2}{p}\right)$ für alle $p|D_0$; zusammen mit $a<0$ geht daher (33) über in

$$\prod_{p|D_0}\left(\frac{2}{p}\right) = -1\,,\quad \text{d.h.}\ \left(\frac{2}{D_0}\right)=-1$$

Für $D\equiv 1 \bmod 8$ ist aber $\left(\frac{2}{D_0}\right)=+1$

3) Im Falle $\boxed{D\equiv 5 \bmod 8}$ hingegen existiert in $\mathcal{C}_0$ ein $\varphi=[a,b,c]$, welches die Forderungen (31) erfüllt. Mit Blick auf obiges Schaloon geht das aus den Betrachtungen des vorigen Punktes 2) leicht hervor, denn im Falle $D\equiv 5 \bmod 8$ ist $\left(\frac{2}{D_0}\right)=\left(\frac{2}{D}\right)=-1$.

4) Sei jetzt $D\equiv 3 \bmod 4$, d.h. $\boxed{D\equiv 3 \text{ oder } 7 \bmod 8}$. Die aus (28) mit dem RZG entspringende Relation lautet

$$(34)\qquad \prod_{p|D_0}\chi_p(\varphi)\cdot\chi_2(\varphi)\cdot\chi_\infty(\varphi) = 1$$

mit χ_2 als dem Charakter $\chi_2(a)=(-1)^{\frac{a-1}{2}}$. Mit (31) sind $\chi_p(\varphi)=1$ für alle $p|D_0$ sowie $\chi_\infty(\varphi)=-1$ vorgeschrieben. Setzt man den einzig verbleibenden Faktor ε_j gleich -1, so ist die Bedingung (30) erfüllt. Folglich existiert ein $\varphi=[a,b,c]\in\mathcal{C}$ mit (31).

5) Auch im Fall $D\equiv 2 \bmod 4$, d.h. $\boxed{D\equiv 2 \text{ oder } 6 \bmod 8}$ existiert ein $\varphi=[a,b,c]\in\mathcal{C}$, das (31) erfüllt. Denn auch für $D\equiv 2 \bmod 4$ hat die Relation (29) die Gestalt (34), nur mit dem Unterschied, daß χ_2 im Falle $D\equiv 2 \bmod 8$ die Gestalt $\chi_2(a)=(-1)^{\frac{a^2-1}{8}}$ und im Falle $D\equiv 6 \bmod 8$ die Gestalt $\chi_2(a)=(-1)^{\frac{a-1}{2}+\frac{a^2-1}{8}}$ hat. Was aber an obiger Argumentation nichts ändert.

|| Mit den oben abgehandelten Beispielen 3), 4) und 5) ist auch die Existenzaussage auf S. $\underline{\text{VI}}$ bewiesen. – Was hier allerdings fehlt –

1) Ferner ist aus den obigen Betrachtungen ohne weiteres ersichtlich: Erfüllt auch $\psi\in\mathcal{C}$ (bzw. $\psi\in\mathcal{C}_0$ im Falle $D\equiv 5 \bmod 8$, d.h. $n\equiv 3 \bmod 8$) die Forderungen (31), so gehört ψ zum selben Geschlecht wie φ (und umgekehrt). Das ist der 1. Schritt von Gauß zur Bestimmung der Anzahl $R_3(n)$ der primitiven Darstellungen $n=x_1^2+x_2^2+x_3^2$. Näher wollen wir hier aber nicht darauf eingehen.

lich ohne Beweis bleibt, ist die Formel (27) für die Anzahl der Geschlechter von $\mathcal{C}$. Sie stellt das Hauptresultat der Gaußschen Theorie der binären Formen dar, zusammen mit dem daraus abgeleiteten Scholion (dessen Inhalt allerdings bei Gauß anders und etwas unübersichtlich formuliert wird). Jedenfalls sagt Gauß mit Recht: "Diese Sätze sind, wenn wir nicht sehr irren, zu den schönsten in der Theorie der binären Formen zu rechnen, umsomehr, weil sie, obwohl sie höchst einfacher Natur sind, doch so versteckt liegen, daß man einen strengen Beweis derselben ohne Unterstützung durch so viele andere Untersuchungen nicht zu erbringen vermag."

vgl. S. XV,

Wenngleich ich hier also die Formel (27) ohne regelrechten Beweis lassen muß, so möchte ich doch wenigstens die Grundzüge des Beweisganges angeben:

1) Am Anfang steht die einfache Feststellung, daß die Gruppe $\mathcal{C}^2$ der Quadrate in $\mathcal{C}$ im Hauptgeschlecht von $\mathcal{C}$ enthalten ist, d.h.

(35) $\mathcal{C}^2 \subseteq \operatorname{Kern} X$

Denn X ist ein Homomorphismus, vgl. (26). Bezeichne nun $\mathfrak{A}$ den Kern des Homomorphismus $\mathcal{C} \to \mathcal{C}^2$, $\varphi \mapsto \varphi^2$. Dann ist also $\mathcal{C} : \mathcal{C}^2 = \#\mathfrak{A}$, und für $\mathfrak{G} = \mathcal{C}/\operatorname{Kern} X$ folgt

(36) $\#\mathfrak{G} = \mathcal{C} : \operatorname{Kern} X$ teilt $\mathcal{C} : \mathcal{C}^2 = \#\mathfrak{A}$, insb. $\#\mathfrak{G} \le \#\mathfrak{A}$

2) Die Untergruppe $\mathfrak{A}$ von $\mathcal{C}$ besteht definitionsgemäß aus allen Klassen $\varphi \in \mathcal{C}$ mit $\varphi^2 = 1$ bzw. $\varphi = \varphi^{-1}$. Mit Blick auf S. XI, Fußnote 1) sind das also genau die Klassen $\varphi = [a,b,c]$, für die $[a,b,c] \simeq [c,b,a] \simeq [a,-b,c]$ gilt.[1] Diese Klassen heißen die

1) bzw. genau jene Klassen, die eine Form φ enthalten, zu der es ein $T \in GL_2(\mathbb{Z})$ mit $\det(T) = -1$ gibt, so daß $\varphi = \varphi \circ T$ gilt; solches φ heißt eine ambige Form.

die „ambigen Klassen" von $\mathcal{C}$. Es ist nun nicht besonders schwer (und jedenfalls völlig elementar), die Ordnung $\#\mathfrak{A}$ von $\mathfrak{A}$ zu bestimmen; wie Gauß ermittelt (vgl. dazu Dirichlet-Dedekind) gilt

(37) $$\#\mathfrak{A} = 2^{\lambda-1}$$

mit λ als Anzahl aller Spezialcharaktere (aller immer zu gegebener Diskriminante D), vgl. S. XIII f. Mit (36) folgt also

(38) $\#\mathfrak{G}$ ist ein Teiler von $2^{\lambda-1}$, insb. $\#\mathfrak{G} \leq 2^{\lambda-1}$

Also mindestens der Hälfte aller denkbaren Charakterwerte, so sagt Gauß in etwa, können keine Geschlechter entsprechen.

Zwischenbemerkung: An dieser Stelle hält Gauß erst einmal inne und leitet aus (38) nochmals das QRG (mitsamt beider Ergänzungssätze) ab. Dieser (in den disquisitiones) zweite Beweis von Gauß dürfte heutzutage weithin unbekannt sein. Er argumentiert (quasi 'juristisch') nur mit Worten, ohne mathematische Formeln. Ich gebe davon eine Kostprobe: Sei eine Primzahl $p \equiv 1 \mod 4$ gegeben. Für $D=p$ ist dann $\lambda=1$, so daß nur der Charakter χ_p zu betrachten ist. Da von der Hauptklasse $\varphi_1=[1,0,p]$ schon der Wert $\chi_p(\varphi_1)=1$ belegt ist, kann es kein $\varphi\in\mathcal{C}$ mit $\chi_p(\varphi)=-1$ geben. Daraus ergibt sich nun folgende Teilaussage des QRG: Ist die Primzahl $q\neq 2$ NQR mod p, so ist p NQR mod q. Wäre nämlich p QR mod q [1], so gäbe es ein φ der Diskriminante p [2], mit $\chi_p(\varphi)=-1$ [3]. Widerspruch! □

---

1) d.h. p ist von der Form $p=b^2-qc$ 2) nämlich $\varphi=[q,b,c]$
3) da ja $\chi_p(\varphi)=\left(\frac{q}{p}\right)=-1$, nach Voraussetzung

Nach dieser Abschweifung zurück zur Formel (27). Zu ihrer Begründung fehlt aber nur, daß – in Umkehrung zu (35) – auch

(39) $$\mathrm{Ker}\,\chi \subseteq \mathcal{C}^2$$

gilt, d.h. daß jede Klasse des Hauptgeschlechts Quadrat einer Klasse von $\mathcal{C}$ ist (oder wie Gauß sagt durch "Duplikation" entsteht). Denn dann hat man insgesamt

(40) $$\mathrm{Ker}\,\chi = \mathcal{C}^2$$ [1]

womit (36) in $\#\mathcal{G} = \mathcal{C} : \mathrm{Ker}\,\chi = \mathcal{C} : \mathcal{C}^2 = \#\mathfrak{A}$ übergeht, wegen (37) also in die gewünschte Formel

(27) $$\#\mathcal{G} = 2^{\lambda-1}$$

Wie ersichtlich ist die Aussage (39) der Kernpunkt der ganzen Sache. Zum Gaußschen Beweis für (39) sagt Dedekind (in D-D.): "Wir können hier unmöglich darauf eingehen, den Beweis mitzuteilen, welchen Gauß auf die Theorie der ternären Formen gestützt hat; da dieses tiefe Theorem aber den schönsten Abschluß der Lehre von der Composition bildet, so können wir es uns nicht versagen, dasselbe .... noch auf einem zweiten Weg abzuleiten...". Was Dedekind dann seinerseits heranzieht, ist der bekannte Satz von Legendre über die Lösbarkeit von Gleichungen der Form $ax^2+by^2+cz^2=0$ (derselbe Satz übrigens, der auch bei Forster und Serre – vgl. Seite I – eine zentrale Rolle spielt).[2] Da Dedekind aber eine gewisse Modifikation dieses Satzes benötigt, wird die Sache selbst bei ihm etwas länglich und weniger übersichtlich als sonst. –

---

1) Es ist wohl diese Aussage, die E. Noether den Gaußschen "Hauptgeschlechtssatz" nennt, wenn sie am 3.6.1932 an H. Hasse schreibt: "Im übrigen habe ich .... einmal Gauß gelesen. Es würde behauptet, daß ein halbwegs gebildeter Mathematiker den Gaußschen Hauptgeschlechtssatz kennt, aber nur Ausnahmemenschen den der Klassenkörpertheorie. Ob das stimmt, weiß ich nicht – meine Kenntnisse gingen in umgekehrter Reihenfolge..."

2) vgl. z.B. F. Lorenz, Algebra II, p.205.

Der Beweis von Gauß für (39) besteht aus zwei Teilen; im ersten greift er auf Betrachtungen zurück, die wir oben schon einmal angesprochen haben, vgl. S. VII f. Es ist der zweite Teil, dem ich nicht folgen konnte, weil Gauß hier auf das Dickicht seiner Formeln zur Composition der Formen verweist. Wie man hier anders zum Ziel gelangen könnte, will ich anschließend skizzieren.

Zum Beweis von (39), erster Teil nach Gauß [1] Gegeben also eine Form bzw. Klasse

$$\varphi = [a, b, c]$$

im Hauptgeschlecht von $\mathcal{C} = \mathcal{C}(D)$; wie stets sei $ggT(a, 2D) = 1$. Aufgrund der Voraussetzung $\varphi \in Kern(\chi)$ ist a QR mod D. Daraus folgt nun genau wie oben bei Üb3, S. VIII: Es existiert eine symm. Matrix $G \in M_3(\mathbb{Z})$ der Gestalt

$$G = \begin{pmatrix} a & b & b_2 \\ b & c & b_3 \\ b_2 & b_3 & a_3 \end{pmatrix} \quad \text{mit } \det(Q) = -1$$

Mit Blick auf Fußnote 1) ist jetzt G indefinit. Nach Gauß (vgl. weiter Art. 277) gibt es bis auf Äquivalenz nur eine indefinite ternäre Form der Determinante -1, nämlich die Form

$$F = X^2 + 2YZ$$

Zu dieser ist G also äquivalent, d.h. es gibt ein $S = \begin{pmatrix} x_1 & x_2 & x_3 \\ y_1 & y_2 & y_3 \\ z_1 & z_2 & z_3 \end{pmatrix} \in SL_3(\mathbb{Z})$ mit $F \circ S = G$, und – analog wie auf S VIII – folgt

$$F(x_1X + y_1Y, x_2X + y_2Y, x_3X + y_3Y) = aX^2 + cY^2 + 2bXY = \varphi,$$

---

1) außerdem ist entweder $D<0$, oder es ist $D<0$ und $a>0$.

d.h. es bestehen die Gleichungen

(41) $a = x_1^2 + 2x_2x_3, \quad b = x_1y_1 + x_2y_3 + x_3y_2, \quad c = y_1^2 + 2y_2y_3$

Wir setzen

(42) $x = x_1y_2 - x_2y_1, \quad y = x_2y_3 - x_3y_2, \quad z = x_3y_1 - x_1y_3$

Mit Blick auf obige Matrix S mit $\det(S) = 1$ ist $ggT(x,y,z) = 1$, und ferner

(43) $y_3x + y_1y + y_2z = 0, \quad x_3x + x_1y + x_2z = 0$

Nach ÜG 1, S. II gilt $\tilde{F}(y,z,x) = -D$, wegen $\tilde{F} = -F$, also

(44) $$D = y^2 + 2xz$$

Wie sich mit (43) leicht ergibt, gilt

(45) x oder z ist <u>ungerade</u>

Sind nämlich x und z beide gerade, so nach (43) auch y_1y und x_1y, wegen $ggT(x,y,z) = 1$ daher auch x_1 und y_1, und nach (41) schließlich auch a und c. Was nicht geht, da φ 1-primitiv ist.

<u>2)</u> Aus den Gleichungen (42) und (41) folgen die Relationen

(46) $x^2 = a y_2^2 + c x_2^2 - 2b x_2 y_2, \quad z^2 = c x_3^2 + a y_3^2 - 2b x_3 y_3$

Indem man hier x_2 durch $-x_2$ bzw. x_3 durch $-x_3$ ersetzt, folgt

(47) φ stellt eine <u>ungerade Quadratzahl</u> s^2 dar

Da wir o.E. gleich von einer <u>primitiven</u> Darstellung von s^2 durch φ ausgehen können, gilt

(48) $\varphi \simeq [s^2, t, u]$ ⌈mit $t, u \in \mathbb{Z}$⌋

Angenommen, s ist prim zu D [1], so sind wir am Ziel. Denn

---

[1] Ein solches s hätten wir, wenn x oder z in (46) prim zu D ist. Ich weiß nicht, ob das der Fall ist.

dann ist s prim zu t (denn $D = t^2 - s^2 u$), also auch zu $2t$ (denn s ist ungerade), und definitionsgemäß (vgl. S. XII) folgt damit

$$[s, t, us] \cdot [s, t, us] = [s^2, t, u] \simeq \varphi ,$$

also ist φ in der Tat das Quadrat einer Klasse von $\mathcal{C}$. Wir haben also die Aussage (47) durch die zusätzliche Forderung zu verschärfen, daß s auch <u>prim zu D</u> ist. Die erwiesene Aussage (47) – etwas anders formuliert – besagt:

(47') φ stellt über $\mathbb{Q}$ die Zahl 1 dar, und zwar 2-adisch ganz, d.h. es gibt ein $v \in \mathbb{Q}^2$ mit

$$\varphi(v) = 1 \quad \text{und} \quad |v|_2 \le 1 ,$$

mit $|\;|_2$ als dem 2-adischen Betrag auf $\mathbb{Q}^2$. Ziel ist zu zeigen, daß auch ein $\tilde{v} \in \mathbb{Q}^2$ mit $\varphi(\tilde{v}) = 1$ existiert, sodaß

(48) $\quad |\tilde{v}|_p \le 1$ für alle $p \in S := \{p | D\} \cup \{p = 2\}$

erfüllt ist. – Vorbereitend stellen wir dazu zunächst fest: Ist p ein ungerader Primteiler von D, so ist a wiegesagt ein QR mod p, und damit auch ein Quadrat in der Einheitengruppe $\mathbb{Z}_p^*$ von $\mathbb{Z}_p$. Dann stellt aber φ offenbar auch 1 über $\mathbb{Z}_p$ dar, und über $\mathbb{Z}_p$ gilt $\varphi \simeq [1, 0, -D]$, wegen $p | D$ also

$$\varphi \simeq X^2 - pd\,Y^2 \quad \text{mit einem } d \in \mathbb{Z}_p$$

Zu jedem $y \in \mathbb{Z}_p$ gibt es nach Hensels Lemma ein $x \in \mathbb{Z}_p$ mit $x^2 - pdy^2 = 1$. Damit sieht man leicht, daß es unter den $v_p \in \mathbb{Z}_p^2$ mit $\varphi(v_p) = 1$ auch eines geben muß, welches

(49) $$\varphi(v, v_p) \neq 1$$

erfüllt (wobei φ auch die zugehörige Bilinearform der quadratischen Form bezeichnet). Dies gilt auch für $p = 2$: Dann folgt aus (47'), daß

φ über $\mathbb{Z}_2$ äquivalent zu $[1,0,-D] = X^2 - DY^2$ ist. Zu jedem $y \in \mathbb{Z}_2$ der Gestalt $y = 4t$, $t \in \mathbb{Z}_2$ gibt es nach Hensels Lemma ein $x \in \mathbb{Z}_2$ mit $x^2 - Dy^2 = 1$. Analog wie oben erkennt man, daß unter den $v_2 \in \mathbb{Z}_2^2$ eines sein muß mit $\varphi(v, v_2) \neq 1$. –

Wir betrachten nun zunächst alle $w \in \mathbb{Q}^2$ mit $\varphi(v,w) \neq 1$ und setzen

$$\lambda = \lambda(w) := \frac{1-\varphi(w)}{2(\varphi(v,w)-1)}$$

Dann gilt $\varphi(\lambda v + w) = (\lambda+1)^2$, also

$$\varphi\left(\frac{\lambda v + w}{\lambda+1}\right) = 1 , \quad \text{falls } \lambda+1 \neq 0$$

Betrachten wir jetzt die $w \in \mathbb{Z}^2$, die für jedes $p \in S$ in $\mathbb{Q}_p^2$ hinreichend nahe bei v_p liegen[1], so ist wegen (49) die Bedingung $\varphi(v,w) \neq 1$ erfüllt und $|\lambda|_p$ ist für jedes $p \in S$ so klein, wie wir nur wollen. Insbesondere können wir $\lambda + 1 \neq 0$ erreichen. Dann erhalten wir mit $\tilde{v} := \frac{\lambda v + w}{\lambda+1}$ aber einen Vektor in $\mathbb{Q}^2$ mit

$$\varphi(\tilde{v}) = 1,$$

der für jedes $p \in S$ so nahe bei v_p liegt, wie wir wollen. Da $v_p \in \mathbb{Z}_p^2$ p-adisch ganz ist für jedes p, so gilt das dann auch für $\tilde{v}$, d.h. $\tilde{v}$ erfüllt wie gewünscht $|\tilde{v}|_p \leq 1$ für alle $p \in S$.

~ Fine ~

---

1) beachte $v_p \in \mathbb{Z}_p^2$. Da $\mathbb{Z}$ dicht in $\mathbb{Z}_p$ ist, folgt die Existenz besagter w mit dem Chinesischen Restsatz.