Werk

Titel: Imaginäre quadratische Zahlkörper mit der Klassenzahl Eins.

Autor: Deuring, M.

Jahr: 1968

PURL: https://resolver.sub.uni-goettingen.de/purl?356556735_0005|log24

Kontakt/Contact

Digizeitschriften e.V.
SUB Göttingen
Platz der Göttinger Sieben 1
37073 Göttingen

info@digizeitschriften.de

Inventiones math. 5, 169–179 (1968)

Imaginäre quadratische Zahlkörper mit der Klassenzahl Eins

MAX DEURING (Göttingen)

Einleitung

STARK hat einen Beweis für den seit langem vermuteten Satz gefunden, daß die einzigen imaginären quadratischen Zahlkörper mit der Klassenzahl 1 die mit den Diskriminanten -3, -4, -8, -11, -19, -43, -67, -163 sind [7]. STARK weist auf die 16 Jahre vor seiner erschienene Arbeit von HEEGNER [3] hin, in der ebenfalls ein Beweis für den in Rede stehenden Satz gegeben wird, der allerdings nicht anerkannt worden zu sein scheint. STARK ist auch der Meinung, daß HEEGNERs Beweis eine Lücke hat, er schreibt: unfortunately, it is thought that there is a gap in HEEGNER's proof, possibly traceable to one of his references, WEBER [8]. Man muß zugeben, daß HEEGNERs Ausführungen nur sehr schwer verständlich sind. STARKs Erfolg und der Umstand, daß er, genau so wie HEEGNER, das Problem auf eine diophantische Gleichung zurückführt, veranlaßten mich, zu versuchen, HEEGNERs Beweis zu verstehen und die vermeintliche Lücke auszufüllen. Beim ersten Lesen gewinnt man den Eindruck, HEEGNER stütze sich auf eine Vermutung von WEBER (vgl. §1), von der er bemerkt, sie lasse sich mittels "algebraischer Untersuchungen im Gebiete zweier Veränderlicher" beweisen, Untersuchungen, über die leider nichts bekannt geworden ist. Ich fand, daß HEEGNERs Beweis durchaus stichhaltig ist und von der Weberschen Vermutung keineswegs Gebrauch macht, wenn von einer ganz geringfügigen Ergänzung abgesehen wird. Der Zweck der vorliegenden Arbeit ist, HEEGNERs Beweis, um jeden Zweifel zu zerstreuen, ganz ausführlich darzustellen.

Der Grundgedanke von HEEGNERs Arbeit ist, kurz gesagt, dieser: Algebraische Gleichungen zwischen Modulfunktionen, die sich aus der Transformationstheorie ergeben (und deren Inhalt im wesentlichen ausmachen), führen, wenn für die Variable eine imaginärquadratische Zahl eingesetzt wird, zu algebraischen Gleichungen zwischen algebraischen Zahlen; da andererseits aus der Klassenkörpertheorie Informationen über diese algebraischen Zahlen folgen, so können die gewonnenen Gleichungen als diophantische Gleichungen in bekannten algebraischen Zahlkörpern angesehen werden. Mit Hilfe der Schlaeflischen Modulfunktion $f(\omega)$ (vgl. §1) kann man mit dieser Methode jedem einklassigen imaginärquadratischen Körper eine ganzrationale Lösung einer diophantischen

Gleichung vom Geschlechte 1 zuordnen. Daß es möglich ist, alle ganzrationalen Lösungen dieser Gleichung zu berechnen, muß wohl noch als ein Zufall angesehen werden; daß ihre Anzahl endlich ist, folgt aus einem allgemeinen Satz von SIEGEL [5] sofort.

Herr SIEGEL zeigt in der an die vorliegende anschließenden Arbeit [6], daß man, statt die Schlaeflische Modulfunktion der Stufe 24 zu benutzen, auch mittels Modulfunktionen der Stufe 5 den einklassigen imaginärquadratischen Körpern Lösungen einer diophantischen Gleichung zuordnen und so den Satz von HEEGNER-STARK beweisen kann. Das scheint zu bestätigen, daß HEEGNERs Ansatz tieferliegende Gründe hat, die aufzuklären eine interessante Aufgabe ist.

Vor HEEGNER und STARK war das schärfste bekannte Resultat über die einklassigen imaginärquadratischen Körper das von HEILBRONN und LINFOOT: außer den neun bekannten Körpern könne es höchstens einen weiteren geben; ob es aber einen solchen zehnten Körper gibt oder nicht, war mit ihrer Methode nicht zu entscheiden [4].

§ 1. Klassische Sätze über singuläre Werte von Modulfunktionen

1. k sei ein imaginärer quadratischer Zahlkörper, er ist durch seine Diskriminante $D(k)=D$ festgelegt. Wenn α eine erzeugende Zahl von k ist $-\ \boldsymbol{Q}(\alpha)=k\ -$, so verstehen wir unter *Diskriminante* $D(\alpha)$ und *Führer* $r(\alpha)$ *von* α Diskriminante und Führer der Ordnung $\mathfrak{o}(\alpha)$ des $\boldsymbol{Z}$-Moduls $[1, \alpha]$ mit der Basis $1, \alpha$; es ist also $D(\alpha)=D\cdot r(\alpha)^2$.

k_r bezeichne den *Ringklassenkörper des Führers* r *von* k, k_r^0 seinen maximalen reellen Teilkörper; insbesondere ist k_1 der Hilbertsche Klassenkörper von k.

2. $j(\omega)$ bedeute die *absolute Invariante* aus der Theorie der Modulfunktionen. Wenn Zahlen α aus k in $j(\omega)$ oder in eine der unten eingeführten Modulfunktionen eingesetzt werden, so soll stillschweigend vorausgesetzt werden, daß $\mathrm{Im}(\alpha)>0$ ist.

Von den Hauptsätzen der Theorie der „Komplexen Multiplikation" brauchen wir

Satz 1. *Für eine erzeugende Zahl* α *von* k *gilt*

$$k(j(\alpha))=k_{r(\alpha)},$$

dabei ist

$$[k(j(\alpha))\colon \boldsymbol{Q}(j(\alpha))]=2;$$

wenn $[1, \alpha]$ *ein Hauptideal der Ordnung* $\mathfrak{o}(\alpha)$ *ist, so ist* $\boldsymbol{Q}(j(\alpha))$ *der maximale reelle Teilkörper* $k^0_{r(\alpha)}$ *von* $k_{r(\alpha)}\cdot j(\alpha)$ *ist eine ganze Zahl.* Vgl. etwa DEURING [1].

WEBER hat in den Abschnitten 19 und 20 des dritten Bandes seines Lehrbuches der Algebra [8] die Frage untersucht, ob nicht $k_{r(\alpha)}$ auch durch

„singuläre Werte" $F(\alpha)$ von anderen Modulfunktionen als $j(\omega)$ erzeugt werden könne; offensichtlich war ihm daran gelegen, möglichst einfache Erzeugungen der Ringklassenkörper zu finden.

Von den zahlreichen Ergebnissen WEBERS in dieser Richtung brauchen wir zwei, die sich auf $j(\omega)^{\frac{1}{3}}$ und auf die *Schlaeflische Modulfunktion* $f(\omega)$ beziehen.

$$\eta(\omega)=e^{\frac{\pi i\omega}{12}}\prod_{n=1}^{\infty}(1-e^{2\pi i n\omega})$$

sei die *Dedekindsche η-Funktion*, die Schlaeflische Funktion f ist dann

$$f(\omega)=e^{-\frac{\pi i}{24}}\frac{\eta\left(\frac{\omega+1}{2}\right)}{\eta(\omega)}=e^{-\frac{\pi i\omega}{24}}\prod_{n=1}^{\infty}(1+e^{2\pi i\omega(n+\frac{1}{2})}).$$

$$\gamma_2(\omega)=(f(\omega)^{24}-16)f(\omega)^{-8} \tag{1}$$

ist eine dritte Wurzel aus $j(\omega)$, $\gamma_2(\omega)^3=j(\omega)$, (vgl. etwa WEBER [8], §§ 24, 34, 54).

WEBER bewies die folgenden beiden Sätze, in denen α eine Erzeugende von k bedeute.

Satz 2. *Die Primzahl* 3 *sei in k unverzweigt, und es sei* $r(\alpha)\not\equiv 0 \bmod 3$, *anders ausgedrückt: es sei* $D(\alpha)\not\equiv 0 \bmod 3$. *Wenn dann außerdem* α *zu* 3 *prim und* $\mathrm{Sp}\,\alpha\equiv 0 \bmod 3$ *ist, so ist*

$$Q(\gamma_2(\alpha))=Q(j(\alpha)).$$

WEBER [8], § 125, S. 459.

Satz 3. *Die Primzahl* 2 *bleibe in k unverzweigt und es sei* $r(\alpha)$ *das Doppelte einer ungeraden Zahl, anders ausgedrückt, es sei* $D(\alpha)\equiv 20 \bmod 32$. *Wenn dann außerdem* α *zu* 2 *prim und* $\mathrm{Sp}\,\alpha\equiv 0 \bmod 8$ *ist, so ist*

$$Q(f(\alpha)^6)=Q(j(\alpha)).$$

WEBER [8], § 127, S. 469.

WEBER vermutete – und bestätigte an vielen Beispielen –, daß unter den Voraussetzungen von Satz 3, und wenn außerdem 2 in k prim bleibt, sogar

$$Q(f(\alpha)^3)=Q(j(\alpha))$$

gilt, WEBER [8], § 127, S. 472.

Satz 4. *Wenn die Voraussetzungen von Satz* 1 *und von Satz* 2 *erfüllt sind, m.a.W., wenn* 2 *und* 3 *in k unverzweigt sind, wenn* $r(\alpha)$ *das Doppelte einer ungeraden Zahl,* α *zu* 6 *prim und* $\mathrm{Sp}\,\alpha\equiv 0 \bmod 24$ *ist, so ist*

$$Q(f(\alpha)^2)=Q(j(\alpha)).$$

Wenn die eben genannte Vermutung richtig ist, gilt sogar $Q(f(\alpha))=Q(j(\alpha))$, 2 in k prim vorausgesetzt.

Beweis. Aus (1) folgt

$$f(\alpha)^2=\frac{f(\alpha)^{24}-16}{\gamma_2(\alpha)\,f(\alpha)^6}$$

denn es ist $f(\alpha)\neq 0$, weil $f(\omega)$ keine Nullstellen hat und $\gamma_2(\omega)=0$ gilt nur, wenn die Zahl ω mit $\frac{-1+\sqrt{-3}}{2}$ nach der Modulgruppe äquivalent ist, also den Körper $k=Q(\sqrt{-3})$ erzeugt, in dem aber 3 verzweigt ist. Da nach Satz 2 $Q(\gamma_2(\alpha))=Q(j(\alpha))$ und nach Satz 3 $Q(f(\alpha)^6)=Q(j(\alpha))$ ist, so folgt $f(\alpha)^2\in Q(j(\alpha))$,

$$Q(j(\alpha))=Q(f(\alpha)^6)\subseteq Q(f(\alpha)^2)\subseteq Q(j(\alpha));\quad Q(f(\alpha)^2)=Q(j(\alpha));$$

und wenn $f(\alpha)^3\in Q(j(\alpha))$, weiter $Q(f(\alpha))=Q(j(\alpha))$.

Satz 5. *Es ist* $[k_2:k_1]=1$, *wenn 2 in k voll zerfällt und für* $D=-3$, $D=-4$; $[k_2:k_1]=2$, *wenn 2 in k verzweigt ist, außer für* $D=-4$; $[k_2:k_1]=3$, *wenn 2 in k prim bleibt, außer für* $D=-3$. *Jeder* k_1*-Primfaktor von 2 ist die* $[k_2:k_1]$*-te Potenz eines* k_2*-Primdivisors.*

Das sind ganz spezielle Aussagen, die sich aus der Kennzeichnung von k_2 als Klassenkörper von k_1 sofort ergeben (DEURING [1]).

§ 2. Heegners Beweis

1. Wir setzen voraus, daß 2 und 3 in k prim bleiben, das läuft darauf hinaus, daß $D\equiv 5 \bmod 8$ und $D\equiv -1 \bmod 3$ ist. $\alpha=\sqrt{D}$ ist dann eine zu 2 und 3 prime Zahl mit dem Führer $r(\alpha)=2$ und der Spur $\mathrm{Sp}\,\alpha=0$. Der Modul $[1,D]$ ist die Ordnung $\mathfrak{o}(\alpha)$ vom Führer 2. Nach Satz 1 ist daher

$$Q(j(\alpha))=k_2^0$$

und nach Satz 4

$$Q(f(\alpha)^2)=Q(j(\alpha))=k_2^0. \tag{2}$$

Wir betrachten die Zahl

$$\beta=\frac{\alpha-1}{\alpha+1}.$$

Es ist

$$\mathrm{Sp}\,\beta=2\cdot\frac{D+1}{D-1}\equiv 0 \bmod 3;$$

β ist zu 2 und zu 3 prim, denn β ist der Quotient der beiden *ganzen* Zahlen

$$\frac{\alpha-1}{2}\quad\text{und}\quad\frac{\alpha+1}{2},$$

deren Normen

$$N\left(\frac{\alpha\pm 1}{2}\right)\equiv -1 \bmod 6$$

sind. Der Modul

$$[1,\beta]=\frac{1}{\alpha-1}[1-\alpha,1+\alpha]=\frac{1}{\alpha-1}\left[1,\frac{1+\sqrt{D}}{2}\right]$$

ist ein *Haupt*ideal der *Haupt*ordnung $\left[1,\frac{1+\sqrt{D}}{2}\right]$ von k. Aus Satz 2 folgt also

$$\boldsymbol{Q}(\gamma_2(\beta))=\boldsymbol{Q}(j(\beta))=k_1^0. \tag{3}$$

2. Bei der Transformation zweiter Stufe

$$\omega\to\frac{\omega-1}{\omega+1}$$

verhält sich $f(\omega)$ so

$$f\left(\frac{\omega-1}{\omega+1}\right)=\sqrt{2}\,f(\omega)^{-1},$$

(was etwa mittels der elementaren Transformationsformeln (WEBER [8], § 34)

$$\eta(\omega+1)=e^{\frac{\pi i}{12}}\eta(\omega);\quad \eta\left(-\frac{1}{\omega}\right)=\sqrt{-i\omega}\,\eta(\omega),\quad \operatorname{Re}\sqrt{-i\omega}>0$$

für die η-Funktion bewiesen werden kann). Wir haben also

$$f(\beta)^2=2\cdot f(\alpha)^{-2}$$

und nach (2)

$$k_2^0=\boldsymbol{Q}(f(\beta)^2)=k_1^0(f(\beta)^2).$$

Weil 2 in k prim bleibt und $k\neq\boldsymbol{Q}(\sqrt{-3})$ ist, so ist $[k_2:k_1]=[k_2^0:k_1^0]=3$ (Satz 5), so daß

$$k_2=k_1(f(\beta)^8)=k_1(f(\beta)^2),\quad k_2^0=k_1^0(f(\beta)^8)=k_1^0(f(\beta)^2)$$

folgt. $f(\beta)^8$ ist Nullstelle des Polynoms

$$F(X)=X^3-\gamma_2(\beta)\,X-16,$$

dessen Koeffizienten wegen (1) und (3) in k_1^0 liegen, $F(X)$ ist also das irreduzible k_1^0-Polynom mit der Nullstelle $f(\beta)^8$, $F(X)=\operatorname{Irr}(f(\beta)^8\,|\,k_1^0)(X)$. Es liegt nahe, jetzt die irreduziblen k_1^0-Polynome für $f(\beta)^4$ und $f(\beta)^2$ zu berechnen, $\operatorname{Irr}(f(\beta)^4\,|\,k_1^0)(X)=G(X)$ und $\operatorname{Irr}(f(\beta)^2\,|\,k_1^0)(X)=H(X)$. Es ist $G(X)G(-X)=-F(X)$, und wenn wir $G(X)=X^3+2AX^2+2BX^2+2C$ mit Koeffizienten aus k_1^0 ansetzen, so ergibt Koeffizientenvergleich

$$B=A^2,\ 4(B^2-2AC)+\gamma_2(\beta)=0,\ C^2=4.$$

Da aber $-C=(N_{k_2^0/k_1^0}f(\beta)^2)^2>0$ ist, so muß $C=-2$ sein. Folglich ist

$$G(X)=X^3+2AX^2+2A^2X-4$$

mit einer Zahl A aus k_1^0, die der Gleichung

$$4A(A^3+4)+\gamma_2(\beta)=0 \tag{4}$$

genügt. In entsprechender Weise ergibt sich

$$H(X)=X^3+2ptX^2+2qX+2t$$

mit p, q, t aus k_1^0 und

$$2(q-p^2t^2)=A,\ 2(q^2-2pt^2)=A^2,\ t^2=1.$$

Wenn wir die in § 1 erwähnte Vermutung WEBERs als richtig voraussetzen, so können wir wie oben auf $t=-1$ schließen. Auf jeden Fall folgt aber

$$H(X)=X^3+2pX^2+2qX+2 \quad \textit{oder} \quad X^3-2pX^2+2qX-2$$

mit zwei Zahlen p und q aus k_1^0, die den Gleichungen

$$A=2(q-p^2),\ A^2=2(q^2-2p) \tag{5}$$

genügen. p und q sind ganze Zahlen: $f(\beta)^8$ (und daher $f(\beta)^2$) ist ganz, weil $F(X)$ ganze Koeffizienten hat $-\gamma_2(\beta)=j(\beta)^{\frac{1}{3}}$ ist nach Satz 1 ganz. Die Primzahl 2 ist in k_1 unverzweigt – in k nach Voraussetzung und weiter in k_1, weil k_1 der Hilbertsche Klassenkörper von k ist. Jeder k_1-Primfaktor von 2 its dritte Potenz *eines* k_2-Primdivisors (Satz 5). Daraus schließen wir, weil $N_{k_2/k_1}(f(\beta)^2)=\pm 2$, also $f(\beta)^2$ durch jeden k_2-Primfaktor von 2 teilbar ist, daß die Koeffizienten von $H(X)$ durch jeden k_1-Primfaktor von 2, also durch 2 teilbar sind, wie behauptet.

Aus (5) folgt durch Elimination von A:

$$(q-2p^2)^2=2p(p^3-1) \tag{6}$$

und aus (4) und (5)

$$\gamma_2(\beta)=-2^5(q-p^2)\big(2(q-p^2)^3+1\big),\ j(\beta)=\gamma_2(\beta)^3. \tag{7}$$

Wir fassen zusammen: *Jedem Körper k, in dem* 2 *und* 3 *prim bleiben, ist eine Lösung der Gl.* (5) *in ganzen Zahlen p, q des Körpers k_1^0 zugeordnet, aus der sich k rückwärts eindeutig bestimmt*, weil die aus (7) zu berechnende Invariante $j(\beta)$ der Hauptklasse der Hauptordnung von k den Körper k festlegt.

3. Wir betrachten jetzt die *einklassigen* Körper k. Wenn 2 oder 3 in k nicht prim bleibt, so ist $-D\leqq 12$. Denn dann muß es in k eine ganze Zahl

$$\xi=a+b\,\frac{D+\sqrt{D}}{2},$$

a, b ganz rational, geben, für die

$$N\xi=\left(a+\frac{Db}{2}\right)^2-b^2\cdot\frac{D}{4}=2 \text{ oder } 3$$

ist, woraus zuerst $b\neq 0$ und weiter $-D\leqq -D\cdot b^2\leqq 12$ folgt.

Für die einklassigen Körper gilt $k_1^0=\boldsymbol{Q}$, daher sind den einklassigen Körpern k mit $D\leqq -12$ *gewisse* ganzrationale Lösungen der Gl. (6) umkehrbar eindeutig zugeordnet. Indem wir $s=q-2p^2$ statt q einführen, geben wir (6) die einfachere Gestalt

$$s^2=2p(p^3-1). \tag{8}$$

Diese diophantische Gleichung vom Geschlechte 1 hat nach einem Satz von SIEGEL [5] nur endlich viele ganzrationale Lösungen, und damit ist schon bewiesen, daß es nur endlich viele einklassige k geben kann. Wir können aber (Satz 7 unten) sämtliche ganzrationalen Lösungen von (8) angeben, nämlich $(p, s)=(0, 0), (1, 0), (-1, \pm 2), (-2, \pm 6)$.

Für $(p, s)=(0, 0)$ finden wir aus (7): $j(\beta)=0$ und für $(p, s)=(-1, -2)$: $j(\beta)=-2^{15}$. Das sind zwar die Invarianten von einklassigen Körpern, aber mit Diskriminanten $D>-12$, denn es ist

$$j\left(\frac{-1+\sqrt{-3}}{2}\right)=0 \quad \text{und} \quad j\left(\frac{-1+\sqrt{-11}}{2}\right)=-2^{15}.$$

Es bleiben vier Lösungen (p, s), denen einklassige Körper mit Diskriminanten <-12 entsprechen *können*, da aber vier solche Körper bekannt sind, die mit den Diskriminanten -19, -43, -67, -163, so kann es einklassige Körper mit Diskriminanten <-163 nicht geben. Damit ist Heegners Beweis beendet:

Satz 6. *Die einklassigen imaginären quadratischen Zahlkörper sind die mit den Diskriminanten* -3, -4, -7, -8, -11, -19, -43, -67, -163.

Die 5 ersten in dieser Reihe sind überhaupt alle Körper mit Diskriminanten >-12. Wir bemerken noch: In $\boldsymbol{Q}(\sqrt{-3})$ ist 3, in $\boldsymbol{Q}(\sqrt{-4})$ und in $\boldsymbol{Q}(\sqrt{-8})$ ist 2 verzweigt, in $\boldsymbol{Q}(\sqrt{-7})$ ist 2 voll zerlegt, in $\boldsymbol{Q}(\sqrt{-8})$ und in $\boldsymbol{Q}(\sqrt{-11})$ ist es 3.

4. Man kann fragen, welchen Lösungen (p, s) von (8) die vier Körper mit den Diskriminanten -19, -43, -67, -163 einzeln entsprechen. Man kann, wie es offenbar HEEGNER meint, die Invarianten $j(\beta)$ nach (7) ausrechnen und mit den bekannten Werten von $j\left(\frac{-1+\sqrt{D}}{2}\right)$ für $D=-19$, -43, -67, -163 vergleichen. Einfacher ist es aber, zu bemerken, daß $-j\left(\frac{-1+ix}{2}\right)$ als Funktion der *positiven* Variablen x mono-

ton steigt, so daß die $j(\beta)$ nur der Größe nach anzuordnen sind. So ergibt sich die Tabelle

$-D$	s	p	q	$-\gamma_2(\beta)$
19	0	1	2	$2^5 \cdot 3$
43	-6	-2	2	$2^6 \cdot 3 \cdot 5$
67	2	-1	4	$2^5 \cdot 3 \cdot 5 \cdot 11$
163	6	-2	14	$2^6 \cdot 3 \cdot 5 \cdot 23 \cdot 29$

Dies dürfte die einfachste Methode zur expliziten Berechnung der vier Werte von $j\left(\frac{-1+\sqrt{D}}{2}\right)$, $D=-19, -43, -67, -163$ sein.

Fragen wir noch, wie sich die beiden Fälle $D=-3$ und $D=-11$ hier einordnen, denen ja auch ganzrationale Lösungen von (8) entsprechen.

Im Falle $D=-11$ gilt nach Satz 4 $\boldsymbol{Q}(f(\sqrt{-11})^2)=k_2^0$, wie für die größeren Diskriminanten. Aber $(\sqrt{-11}-1)(\sqrt{-11}+1)^{-1}$ ist *nicht* zu 3 prim (3 ist in $Q(\sqrt{-11})$ voll zerlegt). Statt dieser Zahl können wir aber $\frac{-3+\sqrt{-11}}{2}$ benutzen. Ziehen wir nämlich die Transformationsformel zweiter Stufe

$$f_2\left(\frac{-3+\omega}{2}\right)=e^{-\frac{\pi i}{8}} \cdot 2^{\frac{1}{4}} f(\omega)^{-1}$$

für die Funktion

$$f_2(\omega)=2^{\frac{1}{4}} \frac{\eta(2\omega)}{\eta(\omega)}$$

heran (WEBER [8], § 128, S. 475) und beachten wir, daß $-f_2(\omega)^8$ ebenso wie $f(\omega)^8$ eine Nullstelle von $X^3-\gamma_2(\omega)X-16$ ist, so folgt, daß hier die positive vierte Wurzel der Nullstelle

$$-f_2\left(\frac{-3+\sqrt{-11}}{2}\right)^8=2^4 f(\sqrt{-11})^{-8}$$

dieses Polynoms, also

$$2f(\sqrt{-11})^{-2},$$

eine Erzeugende des kubischen Körpers k_2^0 ist und die Überlegungen beim Beweis von Satz 6 zeigen, daß auch

$$\gamma_2\left(\frac{-3+\sqrt{-11}}{2}\right)=-2^5(q-p^2)(2(q-p^2)^3+1)$$

mit einer ganzrationalen Lösung (p, q) von (6) sein muß; die Einordnung der Größe nach ergibt den Wert

$$j\left(\frac{-1+\sqrt{-11}}{2}\right)=-2^{15}.$$

Im Falle $D=-3$ ist

$$F(X)=X^3-\gamma_2\left(\frac{-1+\sqrt{-3}}{2}\right)X-16=X^3-16,$$

die reelle Nullstelle $2^{\frac{4}{3}}$ von $F(X)$ und deren positive vierte Wurzel $2^{\frac{1}{3}}$ erzeugen *nicht* k_2^0 (denn es ist $k_2^0=\boldsymbol{Q}$), sondern den maximalen reellen Teilkörper des Strahlklassenkörpers modulo $2\cdot 3$ von $\boldsymbol{Q}(\sqrt{-3})$, wie leicht nachzurechnen ist. Aber die Zuordnung von $\boldsymbol{Q}(\sqrt{-3})$ zu einer rationalen Lösung von (8) läßt sich genau so gewinnen wie in den Fällen $D<-12$.

Für die übrigen einklassigen Körper, in denen 2 nicht prim ist, ist $F(X)$ reduzibel in $\boldsymbol{Q}$:

$$D=-4,\ j(\sqrt{-1})=2^6\cdot 3^3,\ F(X)=X^3-12X-16=(X+2)^2(X-4)$$

$$D=-8,\ j(\sqrt{-2})=2^6\cdot 5^3,\ F(X)=X^3-20X-16=(X+4)(X^2-4X-4)$$

$$=(X+4)(X-2-2\sqrt{2})(X-2+2\sqrt{2})$$

$$D=-7,\ j\left(\frac{-1+\sqrt{-7}}{2}\right)=-3^3\cdot 5^3,\ F(X)=X^3+15X-16$$

$$=(X-1)(X^2+X+16)=(X-1)(X+\tfrac{1}{2}+\tfrac{3}{2}\sqrt{-7})(X+\tfrac{1}{2}-\tfrac{3}{2}\sqrt{-7}).$$

5. **Satz 7.** *Die Gleichung*

$$s^2=2p(p^3-1) \tag{8}$$

hat sechs Lösungen in ganzrationalen Zahlen:

$$(p, s)=(0, 0),\ (1, 0),\ (-1,\ \pm 2),\ (-2, \pm 6).$$

Beweis. Die Lösungen $(p, s)=(0, 0), (1, 0)$ springen in die Augen. Setzen wir jetzt $s\neq 0$ voraus, so sind p und p^3-1 teilerfremd, und wir können vier Fälle unterscheiden: p ist Quadratzahl >1, $-p$ ist Quadratzahl >0, $\pm 2p$ ist Quadratzahl >0.

a) p ist Quadratzahl >1. Dann ist $p^3-1=2v^2$ mit ganzrationalem v, $p^3=(1+v\sqrt{-2})(1-v\sqrt{-2})$. Die beiden Faktoren rechts sind teilerfremd, denn ihre Summe ist 2, sie sind aber zu 2 teilerfremd. Daher ist $1+v\sqrt{-2}=(a+b\sqrt{-2})^3$ mit ganzrationalen a, b; es folgt $1=a(a^2-6b^2)$ und daraus $a=1$, $b=0, p=1$, gegen die Annahme $p>1$; wir erhalten keine neue Lösung von (8).

b) $-p$ ist eine Quadratzahl $q^2>0$. Dann muß $1-p^3=1+q^6=2v^2$ sein mit ganzrationalem v, und q ist ungerade. In der Zerlegung $2v^2=(1+q^2)(\zeta+q^2)(\xi^2+q^2)$, ζ eine primitive dritte Einheitswurzel, sind je zwei der Faktoren rechts teilerfremd, denn die Differenz von je zweien von ihnen ist mit $\sqrt{-3}$ assoziiert, während andererseits $\pm 1\equiv 1+q^2\equiv \zeta+q^2\equiv\zeta^2+q^2 \bmod \sqrt{-3}$ ist. Zwei von diesen Faktoren sind folglich Quadrate in $\boldsymbol{Q}(\sqrt{-3})$, während der dritte das Doppelte eines Quadrates sein muß. Da $\zeta+q^2$ und ξ^2+q^2 konjugiert sind, so folgt

$$\pm(\zeta+q^2)=(a+b\zeta)^2,$$

a und b ganz rational, also

$$\pm 1=b(2a-b),\quad \pm q^2=a^2-b^2.$$

Gilt das obere Vorzeichen, so folgt $b=\pm 1$, $a=\pm 1$, $q=0$, das widerspricht $q\equiv 1 \bmod 2$. Gilt das untere Vorzeichen, so folgt $b=\pm 1$, $a=0$, $q=\pm 1$, das führt zu den beiden Lösungen $(p, s)=(-1, \pm 2)$ von (8).

c) $2p$ ist eine Quadratzahl >0. Dann ist $p^3-1=v^2$ mit ganzrationalem v, $p^3=(1+iv)(1-iv)$. Wäre v ungerade, so wären $1\pm iv$ durch $1+i$, aber nicht durch 2 teilbar, p^3 also durch 2 aber nicht durch 8, Widerspruch. Es ist folglich $1\pm iv\equiv 1 \bmod 2$; und da $(1+iv)+(1-iv)=2$ ist, so sind $1+iv$ und $1-iv$ teilerfremd. Daraus folgt $1+iv=(a+ib)^3$ mit ganzrationalen a, b, $1=a(a^2-3b^2)$, $a=1$, $b=0$, $p=1$, aber $2p=2$ ist keine Quadratzahl; keine neue Lösung von (8).

d) $-2p$ ist eine Quadratzahl >0. Dann folgt

$$1-p^3=v^2,\quad v \text{ ganz rational}.$$

EULER hat bewiesen, daß diese Gleichung an Lösungen in *rationalen* Zahlen nur $p=0$, $v=\pm 1$ und $p=-2$, $v=\pm 3$ hat. $p=0$ scheidet für uns aus, $p=-2$ gibt die beiden letzten Lösungen $(p, s)=(-2, \pm 6)$ von (8). Ein bequem zugänglicher Beweis des Satzes von EULER findet sich in FUETER [2]. Es scheint, daß diese Arbeit von FUETER engere Beziehungen zu den Ansätzen HEEGNERs hat.

Literatur

1. DEURING, M.: Die Klassenkörper der komplexen Multiplikation. Enzykl. d. math. Wiss. I/2, 2. Aufl., Heft 10. Stuttgart: B.G. Teubner 1958.
2. FUETER, R.: Über kubische diophantische Gleichungen. Comm. Math. Helv. **2**, 69–89 (1930).
3. HEEGNER, K.: Diophantische Analysis und Modulfunktionen. Math. Zeitschr. **56**, 227–253 (1952).

4. HEILBRONN, H., and E.H. LINFOOT: On the imaginary quadratic corpora of class-number one. Quat. Journ. Math. (Oxford) **5**, 293—301 (1934).
5. SIEGEL, C.L.: Über einige Anwendungen diophantischer Approximationen. Abh. Preuß. Ak. Wiss. Phys.-math. Kl. 1929, Nr. 1; Ges. Abh. I, S. 209—266. Berlin-Heidelberg-New York: Springer 1966.
6. — Zum Beweise des Starkschen Satzes. Inventiones math. **5**, 180—191 (1968).
7. STARK, H.M.: A complete determination of the complex quadratic fields of class-number one. Michigan Math. Journ. **14**, 1—27 (1967).
8. WEBER, H.: Lehrbuch der Algebra 3, 2. Aufl. Braunschweig: F. Vieweg 1908; Neudruck: New York: Chelsea 1962.

M. DEURING
34 Göttingen
Merkelstraße 45

(Eingegangen am 25. März 1968)