ACTA ARITHMETICA
XXX (1976)

Invarianten des total reellen Körpers siebten Grades mit Minimaldiskriminante

von

MICHAEL POHST (Köln)

0. Einleitung. Betrachtet man total reelle algebraische Zahlkörper vom Grad n mit jeweils kleinstmöglicher Diskriminante d_n, so lassen sich diese für $n = 2, \ldots, 6$ einfach kennzeichnen. Ist n Primzahl ($n = 2, 3, 5$), so erhält man sie als größten reellen Teilkörper des Körpers der $(2n+1)$-ten Einheitswurzeln. Für $n = 4, 6$ entstehen sie durch Adjunktion von $\sqrt{7+2\sqrt{5}}$ beziehungsweise $\cos(2\pi/7)$ aus dem Körper $\boldsymbol{Q}(\sqrt{5})$. Bei $n = 7$ versagt eine solche Kennzeichnung erstmals, denn der größte reelle Teilkörper des Körpers der fünfzehnten Einheitswurzeln besitzt keineswegs den Grad sieben. Der total reelle algebraische Zahlkörper siebten Grades mit Minimaldiskriminante läßt sich daher nur in der Gestalt $F = \boldsymbol{Q}(\varrho)$ angeben, wobei ϱ eine Wurzel des normierten irreduziblen Polynoms

$$f(x) = x^7 + x^6 - 6x^5 - 5x^4 + 8x^3 + 5x^2 - 2x - 1 \tag{1}$$

ist [4]. Seine Diskriminante, sie stimmt mit der Polynomdiskriminante D_f überein, berechnet sich aus den Polynomkoeffizienten zu

$$d_F = 20134393 = 71 \cdot 283583. \tag{2}$$

In dieser Arbeit wird nun F näher erforscht, indem drei Körperinvarianten: Galoisgruppe, Einheitengruppe und Klassenzahl berechnet werden.

1. Das Rechnen in F. Die Rechnungen in F werden unter zweierlei Gesichtspunkten durchgeführt. Zunächst ist F Vektorraum der Dimension $n = 7$ über $\boldsymbol{Q}$. Die Elemente $1, \varrho, \ldots, \varrho^6$ bilden eine Basis, sogar eine Ganzheitsbasis, da Körper- und Polynomdiskriminante übereinstimmen. Jede Zahl z aus F läßt sich also in der Form

$$z = a_1 + a_2\varrho + \ldots + a_7\varrho^6 \quad (a_i \in \boldsymbol{Q},\ i = 1, \ldots, 7) \tag{3}$$

darstellen. Ist z bereits aus $\mathfrak{D}_F$, dem Ring der ganzen Zahlen in F, so stammen die Koeffizienten a_i aus $\boldsymbol{Z}$. Hat man zwei Zahlen y, z aus $\mathfrak{D}_F$ in der Gestalt (3) vorliegen, so lassen sie sich durch ganzzahlige (Integer-) Operationen addieren, subtrahieren, multiplizieren und — falls $y/z \in \mathfrak{D}_F$ — dividieren, indem man komponentenweise verfährt und eventuell auftretende höhere Potenzen ϱ^m ($m \geqslant 7$) mittels (1) reduziert, da ϱ ja Null-

stelle des Polynoms f war. Dieses Vorgehen soll im folgenden „arithmetisches Rechnen" in F heißen.

Schon bei der Division sieht man sich allerdings gezwungen, ein Gleichungssystem zu lösen, was man normalerweise lieber mit einer Gleitkommaarithmetik tun würde. Umständlich wäre auch die Berechnung von Normen und Spuren. Deshalb scheint es vorteilhaft, noch auf eine zweite Art, nämlich mit Gleitkommazahlen — etwa double precision — zu rechnen, was mit „analytisches Rechnen" bezeichnet werden soll. Hierbei wird F als Teilkörper der reellen Zahlen $\boldsymbol{R}$ betrachtet. Das Polynom f besitzt in $\boldsymbol{R}$ sieben reelle Nullstellen, die sich mit dem Verfahren von Newton–Maehly [6] schnell und mit großer Genauigkeit berechnen lassen. Den verschiedenen Nullstellen $\varrho_1 = \varrho$, $\varrho_2, \ldots, \varrho_7$ entsprechen dann die konjugierten Körper $F^{(1)} = F, F^{(2)}, \ldots, F^{(7)}$. Man speichert sinnvollerweise die Werte ϱ_i^j $(i = 1, \ldots, 7;\ j = 1, \ldots, 6)$.

Ist dann etwa $z \in \mathfrak{D}_F$ durch ein Tupel $(a_1, \ldots, a_7)$ ganzer Zahlen gemäß (3) gegeben, so lassen sich die Werte $z^{(i)}$ als reelle Zahlen leicht näherungsweise berechnen und damit auch Norm und Spur von z. Wie bereits erwähnt wird man stets auch Gleichungssysteme — mit der nötigen Vorsicht — „reell" rechnen und die gesuchte Lösung durch Typwandlung (besser: Aufsuchen der nächsten ganzen Zahl) erhalten. Unter das „analytische Rechnen" fällt auch die Bestimmung einer dualen Basis $\omega_1, \ldots, \omega_7$ nebst Konjugierten durch Lösen der Gleichungssysteme

$$\begin{aligned} \mathrm{Sp}(\omega_i \varrho^0) &= \delta_{i1} \\ \mathrm{Sp}(\omega_i \varrho^1) &= \delta_{i2} \qquad (i = 1, \ldots, 7). \\ &\cdots\cdots\cdots \\ \mathrm{Sp}(\omega_i \varrho^6) &= \delta_{i7} \end{aligned}$$

Für die Anwendung der dualen Basis im dritten Abschnitt reichen die erhaltenen Näherungswerte aus.

2. Die Galoisgruppe. Entsprechend der Methode von van der Waerden [7] geht man bei der Bestimmung der Galoisgruppe G_F des Körpers F so vor, daß man das gegebene Polynom f für eine Reihe Primzahlen p modulo p faktorisiert. Die Galoisgruppe von f modulo p ist nämlich Untergruppe von G_F und läßt sich leichter berechnen, weil sie zyklisch ist. Diese Faktorzerlegung von f, für Primzahlen $p < 50$ mit dem Computer durchgeführt, ergibt unter anderem:

$$f(x) \bmod 2 \text{ irreduzibel},$$
$$f(x) \equiv (x^3 + 3x + 19)\,(x^5 + 29x^4 + 12x^3 + 28x^2 + 6x + 13) \bmod 31,$$
$$f(x) \equiv (x + 13)\,(x^6 + 25x^5 + 2x^4 + 6x^3 + 4x^2 + 27x + 17) \bmod 37.$$

Weil $f(x)$ mod 2 irreduzibel ist, muß G_F transitiv sein. Damit sind die Voraussetzungen des folgenden Satzes aus [7] erfüllt:

SATZ. *Eine transitive Permutationsgruppe von n Objekten, die einen Zweierzyklus und einen $(n-1)$-Zyklus enthält, ist die symmetrische Gruppe $\mathfrak{S}_n$.*

Also gilt $G_F = \mathfrak{S}_7$.

Der Nachweis läßt sich noch auf eine weitere Art führen, wenn man

$$f(x) \bmod 3 \text{ irreduzibel},$$
$$f(x) \equiv (x + 2)\,(x^6 + 6x^5 + 3x^4 + 3x^3 + 2x^2 + x + 3) \bmod 7,$$
$$f(x) \equiv (x^3 + 3x^2 + x + 1)\,(x^4 + 3x^3 + 4x^2 + 4x + 4) \bmod 5$$

berücksichtigt. Aus den ersten beiden Zerlegungen folgt, daß G_F transitiv ist und einen Sechserzyklus enthält. Dann ist G_F auch primitiv. Denn wäre G_F imprimitiv, so gäbe es darin ein Primitivitätsgebiet G_1 mit $G_1 \ni a, b$, $a \neq b$ und ein Element $c \notin G_1$. Der unter dem Sechserzyklus fest bleibende Index sei i. Infolge der Transitivität existiert eine Permutation $\sigma \in G_F$ mit $a^\sigma = i$. Weil G_F einen Sechserzyklus enthält, existiert auch eine Permutation $\tau \in G_F$ mit $i^\tau = i$, $b^{\sigma\tau\sigma^{-1}} = c$. Damit folgt aber $a \in G_1 \cap G_1^{\sigma\tau\sigma^{-1}}$ und $c \in G_1^{\sigma\tau\sigma^{-1}} \setminus G_1$ im Widerspruch dazu, daß G_1 Primitivitätsgebiet sein sollte (1).

Wegen der letzten Kongruenz existiert schließlich auch ein Dreierzyklus in G_F; $G_F \geqq \mathfrak{A}_7$ resultiert nach [2], Satz 4.5 in Kapitel II. Andererseits kann $G_F = \mathfrak{A}_7$ nicht gelten, da G_F ungerade Permutationen (Sechserzyklus) enthält. Also muß bereits $G_F = \mathfrak{S}_7$ gelten.

SATZ I. *Die Galoisgruppe des Zerfällungskörpers des Polynoms f aus* (1) *ist die symmetrische Gruppe $\mathfrak{S}_7$.*

3. Die Einheitengruppe. Die Bestimmung der Einheitengruppe eines Zahlkörpers gliedert sich im allgemeinen in zwei Schritte. Zuerst versucht man, ein System unabhängiger Einheiten von Maximalrang zu gewinnen. Hieraus stellt man dann Grundeinheiten her. Der erste Teil ist dabei meist schwieriger. Man hat nämlich Gitterpunkte innerhalb eines abgegrenzten Raumes aufzusuchen, wobei die Abgrenzungen so sind, daß sich das Problem dem rechnerischen Zugriff entzieht. Im konkreten Fall ist es oft besser, „genügend" viele Einheiten — etwa in der Basisdarstellung (3) — zu erzeugen und zu prüfen, ob bereits maximal viele unabhängige darunter sind.

In F liegen die Gegebenheiten günstiger. Bei der Bestimmung der Minimaldiskriminante d_F in [4] traten zwölf Polynome auf, deren Wurzeln alle zu F isomorphe Körper erzeugen. Unter diesen Wurzeln befanden sich nun schon elf Einheiten von F. Aus ihnen ließen sich sechs auswählen, die ein unabhängiges Einheitensystem von maximalem Rang bilden. Allerdings wird sich herausstellen, daß dieses System für die weiteren Rechnungen noch nicht optimal geeignet ist.

(1) Die Primitivität von G_F folgt auch direkt daraus, daß $n = 7$ Primzahl ist.

Aus den sechs unabhängigen Einheiten sollen nun Grundeinheiten gewonnen werden. Das benötigte Kriterium entstammt [3].

„Gehören $\varepsilon_1, \ldots, \varepsilon_k$ $(k = 0, \ldots, 5)$ einem Grundeinheitensystem von F an, so gehört die Einheit ε_{k+1} genau dann ebenfalls zu diesem Grundeinheitensystem, wenn in $\mathfrak{D}_F$ keine Zahl η existiert mit

$$\varepsilon_{k+1} = \pm\varepsilon_1^{m_1}\cdot\ldots\cdot\varepsilon_k^{m_k}\eta^m \quad (m_i, m \in \boldsymbol{Z},\ |m| \geqslant 2,\ 0 \leqslant |m_i| < |m|, \quad i = 1, \ldots, k). \tag{4}$$

Bemerkungen.

(a) Im Spezialfall $k = 0$ erhält man ein Kriterium dafür, ob ε_1 überhaupt einem Grundeinheitensystem angehört. Gleichung (4) lautet hier: $\varepsilon_1 = \pm\eta^m$.

(b) Man überlegt leicht, daß man schärfer $m > 0$ (eventuell Übergang $\eta \to \eta^{-1}$) und $0 \geqslant m_i > -m$, $i = 1, \ldots, k$ (eventuell Übergang $\eta \to \eta\varepsilon_i$) fordern kann.

Im allgemeinen muß sogar $m \equiv 1 \bmod 2$, also $m \geqslant 3$ gelten. Das kann man entscheiden, wenn man (4) auch für die Konjugierten studiert (Vorzeichenvergleich).

Ausgangsbasis für die Rechnungen bilden die bereits erwähnten sechs unabhängigen Einheiten, die in der Gestalt (3) vorliegen und $\varepsilon_1, \ldots, \varepsilon_6$ heißen sollen. Dann ist für $k = 0, \ldots, 5$ festzustellen, ob (4) in $\mathfrak{D}_F$ lösbar ist.

Dazu betrachtet man bei festem k (4) auch für die Konjugierten und erhält die sieben Gleichungen:

$$|\eta^{(i)}|^m = |\varepsilon_1^{(i)-m_1}\cdot\ldots\cdot\varepsilon_k^{(i)-m_k}\varepsilon_{k+1}^{(i)}| \quad (i = 1, \ldots, 7). \tag{5}$$

Hieraus gewinnt man Schranken S_i für die $|\eta^{(i)}|$, indem man

$$\sqrt[m]{|\varepsilon_j^{(i)-m_j}|} \leqslant \begin{cases} 1 & \text{für} \quad |\varepsilon_j^{(i)}| < 1 \\ |\varepsilon_j^{(i)}| & \text{für} \quad |\varepsilon_j^{(i)}| > 1 \end{cases} \quad (j = 1, \ldots, k),$$

sowie

$$\sqrt[m]{|\varepsilon_{k+1}^{(i)}|} \leqslant \begin{cases} 1 & \text{für} \quad |\varepsilon_{k+1}^{(i)}| < 1 \\ \sqrt[3]{|\varepsilon_{k+1}^{(i)}|} & \text{für} \quad |\varepsilon_{k+1}^{(i)}| > 1 \end{cases} \quad \text{(Bemerkung (b))}$$

abschätzt. Setzt man eine mögliche Lösung η von (4) in der Gestalt (3) an:

$$\eta = e_1 + e_2\varrho + \ldots + e_7\varrho^6 \quad (e_j \in \boldsymbol{Z},\ j = 1, \ldots, 7), \tag{6}$$

so folgt durch Multiplikation mit Elementen ω_i $(i = 1, \ldots, 7)$ der dualen Basis von F einerseits nach Definition der dualen Basis

$$\mathrm{Sp}(\eta\omega_i) = \sum_{j=1}^{7} e_j \mathrm{Sp}(\varrho^{j-1}\omega_i) = e_i \tag{7}$$

und zum anderen

$$|\mathrm{Sp}(\eta\omega_i)| \leqslant \sum_{j=1}^{7} |\eta^{(j)}||\omega_i^{(j)}| \leqslant \sum_{j=1}^{7} S_j|\omega_i^{(j)}| =: T_i, \tag{8}$$

indem man die im ersten Abschnitt berechneten Werte für $\omega_i^{(j)}$ einsetzt. (7) und (8) zusammen ergeben nur endlich viele Möglichkeiten für die e_i $(i = 1, \ldots, 7)$ und damit auch für η. Mittels der gespeicherten Werte $\varrho_i^{(j)}$ berechnet man für diese η auf dem Computer alle Konjugierten „analytisch". Ist $|\eta^{(i)}| > S_i$ für ein $i \in \{1, \ldots, 7\}$, wird η eliminiert. Sonst berechnet man durch Produktbildung $N(\eta)$ und überprüft $N(\eta) = \pm 1$. Für verbleibende (Einheiten) η, löst man „analytisch" das Gleichungssystem (5) in logarithmierter Form mit $m_1, \ldots, m_k$, m als Unbekannten. Existiert eine Lösung $m \in \boldsymbol{Z}$, $|m| \geqslant 2$, so untersucht man „arithmetisch", ob (4) mit diesen m, $m_1, \ldots, m_k$, η tatsächlich gilt. In diesem Fall wäre ε_{k+1} durch η zu ersetzen. Existiert dagegen keine Lösung von (4), so erhöht man k um eins und beginnt wieder bei (5).

Schwierigkeiten bei der Durchführung des beschriebenen Verfahrens ergeben sich daraus, daß mit wachsendem k die Schranken T_i für die Koeffizienten e_i so groß werden, daß die Rechenzeit für die Überprüfung der möglichen Zahlen η auf ein nicht mehr vertretbares Maß anwächst. Sind für $k = 0$ etwa 500000 Zahlen η zu betrachten, so wären es bei diesem Vorgehen für $k = 5$ bereits über $2.8 \cdot 10^9$, was viel zu viel Rechenzeit in Anspruch nähme. Versucht man daraufhin, die durchgeführten Abschätzungen zu verbessern, so erkennt man, daß dies in zweierlei Hinsicht möglich ist. Zunächst sind Auswahl und Reihenfolge der zugrunde liegenden unabhängigen Einheiten $\varepsilon_1, \ldots, \varepsilon_6$ wichtig. Die Werte der Konjugiertenbeträge $|\varepsilon_j^{(i)}|$ sollten möglichst klein sein, das heißt im allgemeinen dicht bei eins liegen; je mehr von ihnen dann unterhalb eins liegen, desto besser. Als zweites lassen sich die Schranken S_i verbessern, wenn man bei den Abschätzungen der $\sqrt[m]{|\varepsilon_j^{(i)-m_j}|}$ subtiler vorgeht und etwa die 2^k Fälle $0 \leqslant -m_j < m/2$, $m/2 < -m_j < m$ $(j = 1, \ldots, k)$ unterscheidet. Man erhält:

$$\sqrt[m]{|\varepsilon_j^{(i)-m_j}|} \leqslant \begin{cases} 1 & \text{für} \quad |\varepsilon_j^{(i)}| < 1,\ 0 \leqslant -m_j < m/2, \\ \sqrt{|\varepsilon_j^{(i)}|} & \text{für} \quad |\varepsilon_j^{(i)}| > 1,\ 0 \leqslant -m_j < m/2, \\ \sqrt{|\varepsilon_j^{(i)}|} & \text{für} \quad |\varepsilon_j^{(i)}| < 1,\ m/2 < -m_j < m, \\ |\varepsilon_j^{(i)}| & \text{für} \quad |\varepsilon_j^{(i)}| > 1,\ m/2 < -m_j < m. \end{cases}$$

Eine Unterscheidung in noch mehr Fälle liefert natürlich auch bessere Schranken, wird aber dafür sehr aufwendig.

Betrachtet man die elf gegebenen Einheiten von F und noch weitere, die in den Anlaufrechnungen $(k = 0, 1)$ als Kandidaten η auftreten,

unter dem ersten Gesichtspunkt, so wird man nicht mehr $\varepsilon_1, \ldots, \varepsilon_6$, sondern

$$
\begin{aligned}
\sigma_1 &= -2-4\varrho+4\varrho^2+5\varrho^3-\varrho^4-\varrho^5,\\
\sigma_2 &= -2+\varrho+8\varrho^2-4\varrho^3-6\varrho^4+\varrho^5+\varrho^6,\\
\sigma_3 &= -3+2\varrho+15\varrho^2-4\varrho^3-12\varrho^4+\varrho^5+2\varrho^6,\\
\sigma_4 &= \varrho,\\
\sigma_5 &= -2+\varrho^2,\\
\sigma_6 &= 2+2\varrho-8\varrho^2-\varrho^3+6\varrho^4-\varrho^6
\end{aligned}
\tag{9}
$$

als unabhängige Einheiten auswählen. Der Regulator von $\sigma_1, \ldots, \sigma_6$ beträgt 14.45. Eine untere Abschätzung für den Regulator R von F gestattet es, den Index von $\sigma_1, \ldots, \sigma_6$ in einem Grundeinheitensystem von F zu bestimmen. Die beste mir bekannte Abschätzung [5] liefert $|R| > 0.03627$, der Index ist kleiner oder gleich 398. Mögliche Lösungen von (4) können also bereits eliminiert werden, wenn für sie $m \geqslant 398$ ist.

Mit $\sigma_1, \ldots, \sigma_6$ läßt sich nun das beschriebene Verfahren zur Gewinnung eines Grundeinheitensystems tatsächlich ohne allzu großen Rechenaufwand durchführen. Bemerkenswert erscheint es, daß allein beim sechsten Schritt ($k = 5$) die Unterscheidung in $2^k = 32$ Fälle die Anzahl der möglichen η auf 1/15 der ursprünglichen Anzahl reduziert.

Rechenzeit läßt sich auch noch einsparen, wenn man mehrere Schritte des Verfahrens simultan durchführt. Man berechnet dabei η für die größtmöglichen Schranken und versucht, (4) gleich für mehrere k-Werte zu lösen. Das empfiehlt sich besonders, wenn bereits alle Schranken groß sind, also etwa für $k = 3, 4, 5$. Man erhält schließlich als Resultat:

Satz II. *$\sigma_1, \ldots, \sigma_6$ aus (9) bilden eine Basis der Einheitengruppe des total reellen algebraischen Zahlkörpers siebten Grades mit Minimaldiskriminante.*

4. Die Klassenzahl. Da in jeder Divisorenklasse von F ein ganzer Divisor $\mathfrak{a}$ mit einer Norm

$$
\mathfrak{N}(\mathfrak{a}) \leqslant \left[\frac{7!}{7^7}\sqrt{d_F}\right] = 27 \tag{10}
$$

liegt [1], wird man zunächst die Zerlegung aller Primzahlen $p \leqslant 23$ in Betracht ziehen. Dabei interessieren Primdivisoren von 2 bis zum vierten, von 3 bis zum dritten, von 5 bis zum zweiten und von 7, 11, 13, 17, 19, 23 nur ersten Grades. Ist $\mathfrak{p}$ nun ein Primdivisor vom Grad f, der die Primzahl p teilt, so enthält $\mathfrak{D}_F/\mathfrak{p}$ gerade p^f Elemente, die sich in der Gestalt

$$
\mathfrak{d} = a_1 + a_2\varrho + \ldots + a_f\varrho^{f-1} + \varrho^f \quad \left(a_i \in \left\{-\frac{p-1}{2}, \ldots, +\frac{p-1}{2}\right\}\right. \tag{11}
$$

für ungerade p, $a_i \in \{0, 1\}$ für $p = 2$, $i = 1, \ldots, f$)

repräsentieren lassen. Genau eine dieser Zahlen $\mathfrak{d}$ muß demnach durch $\mathfrak{p}$, ihre Norm durch p^f teilbar sein.

Für die Zerlegung aller Primzahlen $p \leqslant 23$ bietet sich daher folgendes Verfahren an:

Für jedes p berechnet man gemäß Abschnitt 1 die Normen der p^f Zahlen $\mathfrak{d}$ aus (11), wobei f von eins bis zu einer von p abhängigen, oben angegebenen oberen Schranke läuft, und prüft jedesmal, ob $N(\mathfrak{d})$ durch p^f teilbar ist. Für $f = 1$ erhält man so die Existenz von Primdivisoren ersten Grades. Dagegen bestimmt für $f > 1$ nicht unbedingt jede der Zahlen $\mathfrak{d}$ mit $p^f | N(\mathfrak{d})$ einen Primdivisor vom Grad f; falls nämlich Primdivisoren niedrigeren Grades existieren, könnten auch Produkte von ihnen in $\mathfrak{d}$ aufgehen und $p^f | N(\mathfrak{d})$ hervorrufen. Das läßt sich mittels Division in $\mathfrak{D}_F$ (Abschnitt 1) entscheiden.

Es erweist sich als zweckmäßig, die Normen aller Zahlen $\mathfrak{d}$ gemäß (11) für $p = 23$ zu bestimmen und auf Teilbarkeit durch p^f für $p \leqslant 23$ und $f = 1, 2, 3$ zu untersuchen. Für die Zerlegung einer Primzahl $p \leqslant 23$ werden dann jedoch nur solche $\mathfrak{d}$ berücksichtigt, deren Koeffizienten a_i ($i = 1, \ldots, f$) dem absolut kleinsten Restsystem modulo p angehören.

Im ersten Schritt, $f = 1$, erhält man

$$
N(\varrho-8) = 17\cdot 126271, \quad N(\varrho-4) = 23\cdot 593, \quad N(\varrho+2) = 7.
$$

Weitere Zahlen $\mathfrak{d} = \varrho + a_1$ mit $p | N(\mathfrak{d})$ treten nicht auf. Also besitzen genau die Primzahlen 7, 17 und 23 Primdivisoren ersten Grades $\mathfrak{p}_7$, $\mathfrak{p}_{17}$, $\mathfrak{p}_{23}$. $\mathfrak{p}_7 = \varrho + 2$ ist sogar Hauptdivisor.

Für $f = 2$ bekommt man:

$$
N(\varrho^2-10\varrho-8) = 23^2 5231, \quad N(\varrho^2+7\varrho-4) = 17^2 7\cdot 37,
$$
$$
N(\varrho^2+7\varrho-1) = 17^2 2887, \quad N(\varrho^2+3) = 7^2 859
$$

und außerdem

$$
N(\varrho^2-4\varrho+2) = 7^2 17.
$$

Wegen $(\varrho+2) | (\varrho^2+3)$ enthält 7 keinen Primdivisor vom Grad zwei. Ferner hat

$$
\frac{\varrho^2-4\varrho+2}{(\varrho+2)(\varrho+2)} = 4\varrho^6-6\varrho^5-10\varrho^4+8\varrho^3+10\varrho^2-4\varrho-1
$$

die Norm 17. Damit ergibt sich weiter, daß der Primdivisor ersten Grades von 17 die Gestalt

$$
\mathfrak{p}_{17} = 4\varrho^6-6\varrho^5-10\varrho^4+8\varrho^3+10\varrho^2-4\varrho-1
$$

besitzt, also Hauptdivisor ist. Wegen $\mathfrak{p}_{17} | (\varrho^2+7\varrho-1)$ und $\mathfrak{p}_{17} \nmid (\varrho^2+7\varrho-4)$ wird 17 zudem von genau einem Primdivisor zweiten Grades, $\mathfrak{p}_{17,2}$, geteilt. Daher kann 17 nur noch in der Gestalt $17 = \mathfrak{p}_{17}\mathfrak{p}_{17,2}\mathfrak{p}_{17,4}$ mit einem Primdivisor $\mathfrak{p}_{17,4}$ vierten Grades zerfallen.

Schließlich ergeben die Rechnungen für $f = 3$:

$$N(\varrho^3-\varrho^2+8\varrho-2) = 17^3 1613, \quad N(\varrho^3-10\varrho^2+7\varrho-1) = 23^3 7,$$

$$N(\varrho^3-2\varrho^2+\varrho+1) = 5^3, \quad N(\varrho^3-3\varrho^2+2\varrho+3) = 7^3,$$

$$N(\varrho^3-\varrho^2+6\varrho+4) = 13^3 199, \quad N(\varrho^3+3\varrho+8) = 17^3 149,$$

$$N(\varrho^3+9\varrho^2+9\varrho+9) = 23^3 131\cdot 277$$

und zusätzlich

$$N(\varrho^3+3\varrho^2-4\varrho-4) = 5^3 23, \quad N(\varrho^3-\varrho^2-7\varrho+4) = 13^3.$$

Also sind 2, 3, 11, 19 in F träge; denn sie besitzen keine Primdivisoren ersten, zweiten oder dritten Grades. Ferner gilt $5 = \mathfrak{p}_{5,3}\mathfrak{p}_{5,4}$ und $13 = \mathfrak{p}_{13,3}\mathfrak{p}_{13,4}$ mit Hauptdivisoren $\mathfrak{p}_{5,3} = \varrho^3-2\varrho^2+\varrho+1$, $\mathfrak{p}_{13,3} = \varrho^3-\varrho^2-7\varrho+4$ von drittem und $\mathfrak{p}_{5,4}$, $\mathfrak{p}_{13,4}$ von viertem Grade. Wegen $(\varrho+2)\mid(\varrho^3-3\varrho^2+2\varrho+3)$ hat 7 keinen Primdivisor dritten Grades; es gilt $7 = \mathfrak{p}_7\mathfrak{p}_{7,6}$ mit einem Primdivisor sechsten Grades $\mathfrak{p}_{7,6}$. Weiter teilt $\mathfrak{p}_{17}$ die Zahlen $\varrho^3+3\varrho+8$ und $\varrho^3-\varrho^2+8\varrho-2$, was nach den Ergebnissen des zweiten Schrittes zu erwarten war. Schließlich ist

$$\frac{\varrho^3+3\varrho^2-4\varrho-4}{\varrho^3-2\varrho^2+\varrho+1} = 4\varrho^6+2\varrho^5-25\varrho^4-7\varrho^3+37\varrho^2+\varrho-13 = \mathfrak{p}_{23},$$

auch $\mathfrak{p}_{23}$ also Hauptdivisor. Zum Schluß zeigt sich noch $\mathfrak{p}_{23} \nmid (\varrho^2-10\varrho-8)$, $\mathfrak{p}_{23}\mid(\varrho^3-10\varrho^2+7\varrho-1)$ und $\mathfrak{p}_{23}\mid(\varrho^3+9\varrho^2+9\varrho+9)$, so daß 23 genau wie 17 zerlegt ist.

Damit hat man aber nicht nur die Zerlegungen aller Primzahlen $p \leqslant 23$ in F gewonnen, sondern auch

Satz III. *Der total reelle algebraische Zahlkörper siebten Grades mit Minimaldiskriminante besitzt die Klassenzahl* $h = 1$.

Die erforderlichen umfangreichen Rechnungen wurden auf der Anlage Cyber 76 des Rechenzentrums der Universität zu Köln (Abschnitt 2) und über die Datenstation IBM 3780 des Mathematischen Instituts der Universität zu Köln an der IBM 370/165 der Kernforschungsanlage Jülich durchgeführt.

Literatur

[1] Š. J. Borewicz und I. R. Šafarewič, *Zahlentheorie*, Basel und Stuttgart 1966.
[2] B. Huppert, *Endliche Gruppen I*, Berlin, Heidelberg, New York 1967.
[3] T. Nagell, *Contributions à la théorie des modules et des anneaux algébriques*, Arkiv f. Mat. 6 (1965), S. 161–178.

[4] M. Pohst, *The minimum discriminant of totally real seventh degree algebraic number fields*, Erscheint in J. Number Theory.
[5] R. Remak, *Über die Abschätzung des absoluten Betrages des Regulators eines algebraischen Zahlkörpers nach unten*, J. Reine Angew. Math. 167 (1932), S. 360–378.
[6] J. Stoer, *Einführung in die Numerische Mathematik I*, Berlin, Heidelberg, New York 1972.
[7] B. L. van der Waerden, *Algebra I*, Berlin, Heidelberg, New York 1971.

Eingegangen 2. 12. 1974 (645)