On the "Gap" in a Theorem of Heegner

H. M. STARK*

Department of Mathematics,
University of Michigan, Ann Arbor, Michigan 48104

Communicated by D. J. Lewis

Received June 1, 1968

In 1952, Kurt Heegner gave a proof of the fact that there are exactly nine complex quadratic fields of class-number one. His proof rests on the fact that a certain 24th degree polynomial with rational coefficients has a 6th degree factor which also has rational coefficients. Unfortunately, this reducibility has never been justified. In this paper, we fill this gap in Heegner's proof.

1. INTRODUCTION

Recently, Baker [*1*] and Stark [*5*] have independently shown that there are only 9 complex quadratic fields of class-number one. However, in 1952 Heegner [*4*] had already proved the same thing. Unfortunately his proof has been regarded as incorrect or at best, incomplete. We will show here that there is in fact only a very minor gap in Heegner's proof and we will fill this gap.

It will be helpful to have a brief outline of Heegner's proof in our minds before proceeding. Let

$$j(\omega) = \frac{\{1+240\sum_{n=1}^{\infty} \sigma_3(n)\, e^{2\pi i n \omega}\}^3}{e^{2\pi i \omega} \prod_{n=1}^{\infty} (1-e^{2\pi i n \omega})^{24}} \quad (\mathrm{Im}\, \omega > 0) \tag{1}$$

where

$$\sigma_3(n) = \sum_{d|n} d^3.$$

As is well known ([*6*], Section 53), the function j is invariant under the full modular group. Let

$$\gamma_2(\omega) = [j(\omega)]^{\frac{1}{3}}, \tag{2}$$

* The author holds an O.N.R. postdoctoral research associateship.

the cube root being chosen which is real on the imaginary axis. These functions are intimately connected with the theory of binary quadratic forms. Let

$$Q(x, y) = ax^2+bxy+cy^2,\ a > 0,\ (a, b, c) = 1,\ d = b^2-4ac < 0, \tag{3}$$

and let $h(d)$ be the number of such forms which are inequivalent under unimodular substitutions of determinant 1. Then ([6], Section 122),

$$j\left(\frac{-b+\sqrt{d}}{2a}\right)$$

is an algebraic integer of degree (exactly) $h(d)$. In fact if $3|b$, $3\not| d$ then

$$\gamma_2\left(\frac{-b+\sqrt{d}}{2a}\right)$$

is also an algebraic integer of degree $h(d)$ (instead of the expected $3h(d)$). This is the first of a series of remarkable occurrences whereby the degrees of certain algebraic integers turn out to be less than what one might reasonably expect them to be.

For the rest of Sections 1 and 2, let d be a negative field discriminant, $|d| \equiv 3(\text{mod}\, 8)$, $3\not| d$. In this case $h(d)$ is also the class number of the field, $Q(\sqrt{d})$. Let

$$f(\omega) = e^{-(\pi i\omega)/24} \prod_{n=1}^{\infty} (1+e^{(2n-1)\pi i\omega}). \tag{4}$$

Then ([6], Section 54), $f(\omega)$ satisfies the equation

$$x^{24}-\gamma_2(\omega)x^8-16 = 0. \tag{5}$$

When

$$\omega = \frac{-3+(d)^{\frac{1}{2}}}{2},$$

Heegner states, without proof, that there is a sixth degree factor of (5) whose coefficients are algebraic integers of degree $h(d)$. Heegner finds a relation between these coefficients; in the case of $h(d) = 1$, he gets a Diophantine equation involving rational integers which he can solve. The solutions all correspond to known fields.

In Section 2 we will give a complete account of Heegner's proof including the crucial result that his algebraic integers are of the correct degree. This is all based on the material of Weber [6]. In Section 3 we discuss the validity of Weber's proofs (this is important because there is a widely held view that the trouble in Heegner may be ultimately traced to Weber). Finally in the last section, we go contrary to the modern trend and eliminate all but the most elementary algebraic number theory from this method. Lastly, many people have been studying Heegner's work. Birch has independently come to the conclusion that Heegner's proof can be made correct. His work will appear soon [2].

2. Heegner's Proof

The key to the reducibility of (5) lies with another root of (5). Let

$$f_2(\omega) = \sqrt{2}\, e^{\pi i\omega/12} \prod_{n=1}^{\infty} (1+e^{2n\pi i\omega}). \tag{6}$$

Then $e^{\pi i/8} f_2(\omega)$ is also a root of (5) and this is the important root of (5). To simplify our notation, let

$$\begin{gathered} J = j(\sqrt{d}),\ F = f(\sqrt{d}),\ h = h(d), \\ j = j\left(\frac{-3+(d)^{\frac{1}{2}}}{2}\right), f = e^{\pi i/8} f_2\left(\frac{-3+(d)^{\frac{1}{2}}}{2}\right),\ \gamma = \gamma_2\left(\frac{-3+(d)^{\frac{1}{2}}}{2}\right). \end{gathered} \tag{7}$$

The relationship between f and F is given by Weber ([6], Section 128):

$$f^2 = \frac{2}{F^2}. \tag{8}$$

Weber proves ([6], Section 127) that F^2 is in the field $Q(J)$. He conjectures that F is also, but is unable to prove this fact. Heegner uses this result elsewhere in his paper but it is not necessary to the class-number one problem; however, it may be the source for blaming the trouble on Weber. Thus

$$Q(f^2) = Q(F^2) = Q(J); \tag{9}$$

the last part is because J may be expressed in terms of F^2 from (2) and (5).

Now, there is a cubic transformation equation relating J and j ([6], Section 69) (which we give explicitly in Section 4) of the form

$$J^3 + rJ^2 + sJ + t = 0,$$

where r, s, t are in $Q(j)$. Thus

$$[Q(j, J) : Q] = [Q(j, J) : Q(j)] \cdot [Q(j) : Q] \leq 3h. \tag{10}$$

But on the other hand,

$$[Q(j, J) : Q] \geq [Q(J) : Q] = 3h \tag{11}$$

since when $|d| \equiv 3 (\text{mod } 8)$ and $d \neq -3$, we have $h(4d) = 3h(d) = 3h$ ([3], p. 138). It follows from (10) and (11) that $Q(J) = Q(J, j)$ is a cubic extension of $Q(j)$ and thus $Q(f^2)$ is a cubic extension of $Q(j)$. Therefore f^2 satisfies a unique equation of the form

$$x^3 + \lambda x^2 + \mu x + \nu = 0, \tag{12}$$

where λ, μ, ν are in $Q(j)$ and in fact are integers in $Q(j)$ since f^2 is an integer (this follows from (5) since γ is an integer). By transposing even degree terms of (12) and squaring, we get an equation for f^4:

$$x^3+\delta x^2+\varepsilon x+\phi = 0,$$

where

$$\delta = 2\mu-\lambda^2,\ \varepsilon = \mu^2-2\lambda\nu,\ \phi = -\nu^2. \tag{13}$$

Repeating this process we get an equation for f^8:

$$x^3+(2\varepsilon-\delta^2)x^2+(\varepsilon^2-2\delta\phi)x-\phi^2 = 0. \tag{14}$$

But since here $Q(f^8) = Q(f^2)$, we see that equation (14) is unique and we already know it to be

$$x^3-\gamma x-16 = 0.$$

Hence $\varepsilon^2-2\delta\phi = -\gamma$ and more importantly,

$$\delta^2 = 2\varepsilon,\ \phi^2 = 16. \tag{15}$$

Since $(d)^{\frac{1}{2}}$ is purely imaginary, J is real and hence ν is real. Therefore $\phi = -\nu^2 \leq 0$ and hence $\phi = -4$, $\nu = \pm 2$. It then follows from (15) and (13) that

$$(2\mu-\lambda^2)^2 = 2(\mu^2\pm 4\lambda), \tag{16}$$

and this gives us a Diophantine equation with entries in $Q(j)$ as desired.

To see how this leads to a solution to the class-number one problem, we note that when $h(d) = 1$, $d < -8$, we have $3\not| d$ and $|d| \equiv 3 (\mathrm{mod}\ 8)$ ([3], p. 184). Thus (16) holds with μ and ν being rational integers. Hence λ is even and as a consequence, so is μ. Let

$$\pm\lambda = 2\alpha,\ \mu = 2\beta. \tag{17}$$

Putting this in (16) finally yields

$$2\alpha(\alpha^3+1) = (\beta-2\alpha^2)^2. \tag{18}$$

This is Heegner's Diophantine equation. Equation (18) is easily solved, the solutions are

$$(\alpha, \beta) = (0, 0), (1, 0), (-1, 2), (2, 2), (1, 4), (2, 14).$$

We may calculate γ from these values of α and β getting respectively

$$\gamma = 0,\ -32,\ -96,\ -960,\ -5280,\ -640320,$$

which correspond uniquely to

$$d = -3,\ -11,\ -19,\ -43,\ -67,\ -163, \text{ respectively.}$$

3. The Critical Result of Weber

Most of the material in Weber is not pertinent to the problem at hand and the pertinent material is scattered throughout the book. To make matters worse, Weber has many little errors and omissions such as failing to prove that the coefficients of a modular function are rational but these may all be filled by the patient reader. But there is one point in the critical result that F^2 is in $Q(J)$ where Weber may be said to have an incomplete proof that is not easily filled. However, at this point, an alternate proof may be given which is more in line with Weber's own proofs of similar results. As this is the only real difficulty in the pertinent material of Weber, we will restrict our attention to this one point in this section.

The roots of the equation

$$(x-16)^3 = xj(\omega) \tag{19}$$

are $f(\omega)^{24}$, $-f_1(\omega)^{24}$, $-f_2(\omega)^{24}$ where f and f_2 are given in (4) and (6) and

$$f_1(\omega) = e^{-(\pi i\omega)/24}\prod_{n=1}^{\infty}(1-e^{(2n-1)\pi i\omega}).$$

Alternatively, the roots of (19) may be given as ([6], Section 126) $f(\omega)^{24}$, $f(\omega+1)^{24}$, $f(1-(1/\omega))^{24}$ and this is the more useful formulation here. Let

$$x = f(\omega)^{24},\ v = f\left(\frac{r\omega+s}{t}\right)^{24},$$

where

$$rt = n > 0,\ n \text{ odd},\ r > 0,\ s \equiv 0 \left(\text{mod}\begin{cases}16 \text{ if } 3\,|\,n\\ 48 \text{ if } 3\nmid n\end{cases}\right). \tag{20}$$

Then there is a transformation equation

$$\Phi_n(x, v) = 0$$

relating x and v. Here $\Phi_n(x, v)$ is a polynomial in x and v with rational coefficients and all the solutions to the equation in v,

$$\Phi_n(f(\omega)^{24}, v) = 0,$$

are given by

$$v = f\left(\frac{r\omega+s}{t}\right)^{24}$$

for some choice of r, s, t satisfying (20). We will return to this point shortly; let us see in the meantime how Weber uses this result.

Suppose $x \neq 0$ is a root of the equation

$$\Phi_n(x, x) = 0. \tag{21}$$

Then there is an ω in the upper half plane such that $x = f(\omega)^{24}$. Thus for some r, s, t satisfying (20),

$$f(\omega)^{24} = f\left(\frac{r\omega+s}{t}\right)^{24}.$$

Weber shows in Section 126 that this requires ω to be the root of a quadratic equation with integral coefficients whose middle coefficient is even and whose outer coefficients are odd. Let

$$\theta = \frac{-b+(d)^{\frac{1}{2}}}{2a}, \tag{22}$$

where a, b, d are given in (3) and d is no longer restricted to fundamental discriminants. Weber shows that if $2|b$ and

$$f(\theta)^{24} = f\left(\frac{r\theta+s}{t}\right)^{24},$$

where

$$rt = n \text{ is odd} > 0,\ r > 0,\ s \equiv 0 \left(\bmod\ \begin{matrix} 16 \text{ if } 3\,|\,n \\ 48 \text{ if } 3\nmid n \end{matrix}\right)$$

then a and c are both odd. While Weber does not show it, it is easy to see that there exists n, r, s, t such that the converse holds.

The quadratic equations satisfied by θ, $\theta+1$, $1-1/\theta$ are

$$\begin{aligned} &ax^2+bx+c = 0, \\ &ax^2+(b-2a)x+(a-b+c) = 0, \\ &cx^2-(b+2c)x+(a+b+c) = 0, \end{aligned}$$

respectively. If a and c are both odd and b even then only $f(\theta)^{24}$ of the three numbers $f(\theta)^{24}, f(\theta+1)^{24}, f(1-1/\theta)^{24}$ can be a root of (21) and for the proper choice of $n, f(\theta)^{24}$ will be a root of (21). But then (19) and (21) have only the root $f(\theta)^{24}$ in common and by the Euclidean algorithm, $f(\theta)^{24}$ can be rationally expressed in terms of $j(\theta)$, that is, $f(\theta)^{24}$ is in $Q(j(\theta))$. It follows from (5) that if $3|b$, $3\nmid d$ also, then $f(\theta)^8$ is in $Q(j(\theta))$ since now $\gamma_2(\theta) \neq 0$ is in $Q(j(\theta))$.

Let

$$x = f(\omega)^3,\ v = f\left(\frac{r\omega+s}{t}\right)^3,$$

where r, s, t satisfy (20). Here again there is a transformation equation

$$\Phi_n(x, v) = 0$$

relating x and v with rational coefficients such that the roots of the equation in v,

$$\Phi_n(f(\omega)^3, v) = 0$$

are all of the form

$$v = f\left(\frac{r\omega+s}{t}\right)^3,$$

where r, s, t satisfy (20).

Let $x \neq 0$ be a solution of the equation

$$\Phi_n(x, x) = 0.$$

Then there is an ω in the upper half plane such that

$$x = f(\omega)^3,$$

and for this ω we have

$$f(\omega)^3 = f\left(\frac{r\omega+s}{t}\right)^3.$$

Suppose $m \equiv 3 \pmod 4$, $m > 0$, and θ is given by (22) and (3) with

$$d = -4m.$$

If ac is odd and $16|b$ then $\mathrm{f}(\theta)^3$ is a root of

$$\Phi_m(x, x) = 0, \tag{23}$$

and conversely if a is odd, and $f(\theta)^3$ is a root of (23) then c is odd and $16|b$. Suppose ac is odd and $16|b$. The eight roots of

$$x^8 - f(\theta)^{24} = 0 \tag{24}$$

are $f(\theta+2k)^3$, $0 \leq k \leq 7$. The corresponding reduced quadratic equation for $\theta+2k$ is

$$ax^2+(b-4ak)x+(c-2kb+4ak^2) = 0,$$

and the only equations with $16|(b-4ak)$ are with $k = 0, 4$. Thus (23) has the two roots $f(\theta)^3$ and $f(\theta+8)^3 = -f(\theta)^3$ in common with (24) and thus $x^2 - f(\theta)^6$ is the greatest common divisor of (23) and (24). Hence $f(\theta)^6$ may be found in terms of $f(\theta)^{24}$ and rational numbers by means of the Euclidean algorithm, that is, $f(\theta)^6$ is in $Q(j(\theta))$ also. Hence if $3 \nmid d$, ac is odd and $48|b$ then $f(\theta)^2 = f(\theta)^8/f(\theta)^6$ is also in $Q(j(\theta))$. This shows how Weber proves that F^2 is in $Q(J)$ and the role of the transformation equations in this proof.

Now let us examine these transformation equations themselves. It is here that a difficulty arises, but it is one that may be eliminated by a choice of a different transformation equation. Weber uses Schlafli's modular equation for his transformation equation. Let

$$u = f(\omega),\ v = f\left(\frac{r\omega+s}{t}\right),$$

where $rt = n$ is an odd positive integer, $r > 0$, $16|s$ and if $3 \nmid n$ then $48|s$. Let

$$A = \left(\frac{u}{v}\right)^k + \left(\frac{v}{u}\right)^k,\ B = (uv)^l + \left(\frac{2}{n}\right)^{k+l} \cdot \frac{2^l}{(uv)^l},$$

where $(2/n)$ is a Jacobi symbol and k and l are rational integers which satisfy the conditions

$$\frac{n-1}{12}k \equiv \frac{(n+1)l}{12} \pmod 2.$$

Weber shows in Section 73 that there is a polynomial relation between A and B with rational coefficients (dependent on n but independent of

r, s, t) and this is known as Schlafli's modular equation,

$$\phi_n(u, v) = 0.$$

However, when we clear the denominator of v, we have no guarantee from Weber that the degree of $\phi_n(u, v)$ in v is such that

$$\phi_n(u, v) = 0$$

implies

$$v^g \equiv f\left(\frac{r\omega+s}{t}\right)^g$$

for some choice of r, s, t satisfying all the above conditions (here $g = 24$ or 3 according to which application we have in mind).

Since extra roots would ruin everything, we form a different transformation equation which is more in line with the type Weber uses for $j(\omega)$ and $\gamma_2(\omega)$. Consider the set of functions

$$f\left(\frac{r\omega+s}{t}\right)^k f(\omega)^{23nk}$$

with n and k fixed positive integers, $3|k$, n odd, and r, s, t are variable integers such that

$$r > 0,\ 16|s,\ 0 \leq s < 16t,\ rt = n,\ (r, s, t) = 1.$$

The material of Section 73 of Weber shows us that these functions are permuted among themselves under the transformations

$$\omega \rightarrow \omega+2 \quad \text{and} \quad \omega \rightarrow \frac{-1}{\omega}.$$

Since these two transformations generate the subgroup, G, of the modular group fixing $f(\omega)^{24}$, the coefficients of the powers of x in

$$\prod_{r,s,t}\left[x - f\left(\frac{r\omega+s}{t}\right)^k f(\omega)^{23nk}\right] = \sigma_n(x, f(\omega)^{24}), \tag{25}$$

(where the product is over r, s, t such that $rt = n$, $r > 0$, $0 \leq s < 16$t, $16|s$, and $(r, s, t) = 1$), are invariant under G.

A fundamental domain for G may be taken so that its only parabolic cusps are at 1 and $i\infty$. As $\omega \rightarrow 1$, through such a fundamental domain, $f(\omega) \rightarrow 0$. Further $f((r\omega+s)/t) \rightarrow 0$ as $\omega \rightarrow 1$ (through a fundamental domain for G) for $rt = n$ odd and s even. To demonstrate this, let

$$(r+s, t) = e,$$

and set

$$\gamma = \frac{-t}{e},\ \delta = \frac{r+s}{e}.$$

Then $(\gamma, \delta) = 1$ and thus there are integers α and β such that

$$\alpha\delta - \beta\gamma = 1.$$

Since γ and δ are both odd, we see from Section 40 of Weber that

$$f\left(\frac{r\omega+s}{t}\right)^{24} = -f_2\left(\frac{\alpha((r\omega+s)/t)+\beta}{\gamma((r\omega+s)/t)+\delta}\right)^{24} = -f_2\left(\frac{\alpha er\omega+\alpha es+\beta et}{tr(1-\omega)}\right)^{24},$$

and since $f_2(\omega) \to 0$ as $\omega \to i\infty$ in any vertical strip, $f((r\omega+s)/t) \to 0$ as $\omega \to 1$ through a fundamental domain for G.

At $i\infty$, the coefficients of the powers of x are series in fractional powers of $q = e^{\pi i\omega}$. Thus as $\omega \to i\infty$ the coefficients of the various powers of x each approach definite limits (possibly infinite). Hence the coefficients of the powers of x are automorphic functions, invariant under the group G fixing $f(\omega)^{24}$ and which are finite in the upper half plane and the parabolic cusp at $\omega = 1$. Therefore, the coefficients of each power of x are polynomials in $f(\omega)^{24}$. In other words $\sigma_n(x, y)$ as defined by (16) is a polynomial in two variables. The coefficients in $\sigma_n(x, y)$ will be rational numbers if the series expansion in $q = e^{\pi i\omega}$ of the coefficients of x in (25) have rational coefficients. But this is true as we shall now show.

Consider the product

$$\prod_{\substack{s \\ 0 \le s < 16t \\ 16|s \\ (r,s,t)=1}} \left[x - f\left(\frac{r\omega+s}{t}\right)^k f(\omega)^{23nk}\right], \tag{26}$$

where r and t are fixed, $rt = n$, $r > 0$. Now as we see from (4), $f(\omega)^k$ has a series expansion in integral powers of $q = e^{\pi i\omega/8}$ (recall that $3|k$) all of whose coefficients are rational numbers. Thus $f[(r\omega+s)/t]$ has a series expansion in integral powers of $\zeta^{s/16}q^{r/t}$ where

$$\zeta = e^{2\pi i/t}$$

is a primitive tth root of unity. Suppose we replace ζ in this expansion by ζ^l where $(l, t) = 1$. Define s' to be the unique integer in the range $0 \le s' < 16t$ such that $16|s'$ and $ls/16 \equiv s'/16 \pmod{t}$. Since $(l, t) = 1$, different values of s give different values of s'. Also since t is odd and $(l, t) = 1$,

$$\begin{aligned}(r, s', t) &= (r, (s', t)) = (r, (s'/16, t)) = (r, (s/16, t)) \\ &= (r, (s, t)) = (r, s, t) = 1.\end{aligned}$$

Lastly $\zeta^{ls/16} = \zeta^{s'/16}$ and hence if we replace ζ by ζ^l in the q-expansion of $f[(r\omega+s)/t]$, we merely get $f[(r\omega+s')/t]$. Thus the factors in the above product merely permute with one another when we replace ζ by any of its conjugates and hence the series in fractional powers of q which results as the coefficient of a given power of x in the above product has rational coefficients. Thus when we multiply the various products of the type in (26) together to get (25), the coefficients of the powers of x will be series in (possibly fractional) powers of $q = e^{\pi i\omega}$ with rational coefficients. Since these series are actually automorphic functions on the group preserving $f(\omega)^{24}$, they are actually series in integral powers of $q = e^{\pi i\omega}$ with rational coefficients and thus they are expressible as polynomials in $f(\omega)^{24}$ with rational coefficients. Hence $\sigma_n(x, y)$ is a polynomial in $\mathbf{Z}[x, y]$.

Suppose now that in addition to having $3|k$, we also have $k|24$. Let

$$\Phi_n(x, y) = \sigma_n(xy^{23n}, y^{24/k}). \tag{27}$$

Then $\Phi_n(x, y)$ is a polynomial in $\mathbf{Z}[x, y]$. Let us investigate the roots of the equation

$$\Phi_n(x, x) = 0. \tag{28}$$

Since $f(\omega) \neq 0$ for ω in the upper half plane, the root $x = 0$, if it occurs of (28) is uninteresting and thus, let us suppose that $x \neq 0$ is a root of (28). Then there exists an ω in the upper half plane such that

$$x = f(\omega)^k. \tag{29}$$

Comparing (27) and (28); this means that (29) also provides a solution for x in

$$\sigma_n(xf(\omega)^{23nk}, f(\omega)^{24}) = 0.$$

It follows from (25) that for some set of integers r, s, t satisfying the restrictions of (25),

$$xf(\omega)^{23nk} = f\left(\frac{r\omega+s}{t}\right)^k f(\omega)^{23nk}$$

and since

$$f(\omega)^k = x \neq 0,$$

$$f(\omega)^k = x = f\left(\frac{r\omega+s}{t}\right)^k.$$

Thus we have produced a transformation equation which answers our objections to the one used by Weber.

4. The Elimination of Algebraic Number Theory

When we trace through everything in Weber that is necessary to justify the reduction of (5), we find that with one exception, the algebraic number theory required is minimal. Nothing more advanced is required than what was used to justify that $\sigma_n(x, f(\omega)^{24})$ in (25) has rational coefficients. The exception is found in showing that $j(\theta)$ has degree exactly $h(d)$, it being easy to show that the degree of $j(\theta)$ is less than or equal to $h(d)$.

Here a large amount of algebraic machinery, bordering on class field theory, is necessary to achieve the result. But if $-d \equiv 3 \pmod 8$, and $h(d) = 1$, it is then trivial that

$$j = j\left(\frac{-3+(d)^{\frac{1}{2}}}{2}\right) = j\left(\frac{-1+(d)^{\frac{1}{2}}}{2}\right)$$

is of degree $h(d)$ and it may be shown (without the use of class field theory) that for sufficiently large $|d|$, $J = j(\sqrt{d})$ is of degree 3 ($= h(4d)$). As long as we can find a definite bound on "sufficiently large," this will clearly be sufficient for our purposes.

Suppose $-d \equiv 3 \pmod 8$ and $h(d) = 1$. Then $h(4d) = 3$ and thus J will be of degree 3 if we can show that J is neither rational nor in a quadratic field. There is a cubic equation with rational coefficients relating j and J; J is a root of the invariant equation

$$F_2(x, j) = 0 \tag{30}$$

given by ([6], Section 69),

$$F_2(x, j) = (x-J)\left(x-j\left(\frac{-1+(d)^{\frac{1}{2}}}{4}\right)\right)\left(x-j\left(\frac{1+(d)^{\frac{1}{2}}}{4}\right)\right).$$

If J is either rational or quadratic then (30) has a rational root. But for $|d| > 16$, $j[(\pm 1+(d)^{\frac{1}{2}})/4]$ is in the interior of the usual fundamental domain for $j(\omega)$ and hence $j[(\pm 1+(d)^{\frac{1}{2}})/4]$ is not even real let alone rational. Thus the rational root of (30) must be J. If we set

$$t = e^{2\pi i(-1+\sqrt{d})/2},$$

then

$$j = 1/t + 744 + 196884t + 21493760t^2 + O(t^3),$$
$$J = 1/t^2 + 744 + 196884t^2 + O(t^4),$$

where O refers to $t \to 0$, or alternately, $d \to -\infty$. Hence

$$j^2 - 1488j + 160512 - J = 42987520t + O(t^2). \tag{31}$$

But the left side of (31) is supposedly a rational integer while for a large value of $|d|$, the right side of (31) is strictly between 0 and 1. Here "large" is definitely determinable and a little calculation shows that $|d| > 60$ is already too large. Thus all but the simplest algebraic number theory may be eliminated from the Heegner approach to the class-number one problem.

5. Conclusion

As may be seen in [6], Section 128, Weber knew that equations such as (5) could be reduced under certain circumstances to equations of lower degree with rational coefficients. Since this immediately follows the section ([6], Section 127) where Weber proves that F^2 is in $Q(J)$, one can have little doubt but that Weber could have justified the reduction had he seen any need to do so. Thus had he only made the observation that the reducibility of (5) would lead to a Diophantine equation, the class-number one problem would have been solved 60 years ago.

Note added in proof. Max Deuring has also filled the gap in Heegner's paper. See his article, Imaginäre quadratische Zahlkörper mit der Hlassenzahl Eins, *Inventiones Math.* **5** (1968), 180–191. Deuring uses Weber's result that F^2 is in $Q(J)$ without comment; Birch reproves this result as well as Weber's conjecture that F is in $Q(J)$. Both Birch and Deuring use classified theory.

REFERENCES

1. BAKER, A. Linear forms in the logarithms of algebraic numbers. *Mathematika* **13** (1966), 204–216.

2. BIRCH, B. J. To appear.

3. DICKSON, L. E. "History of the Theory of Numbers", Vol. 3. Stechert, New York, 1934.

4. HEEGNER, K. Diophantische analysis und modulfunktionen. *Math Z.* **56** (1952), 227–253.

5. STARK, H. M. A complete determination of the complex quadratic fields of class-number one. *Mich. Math. J.* **14** (1967), 1–27.

6. WEBER, H. "Lehrbuch der Algebra", Vol. 3. Chelsea, New York, 1961.