

## Conspectus materiae tomi XXII, fasciculi 2

	Pagina
P. J. Weinberger, Exponents of the class groups of complex quadratic fields	117
Donald L. McQuillan, A remark on Hilbert's Theorem 92	125
R. Scharck und J. M. Wills, Asymptotisches Verhalten einer diophantischen Approximations-Funktion	129
François Dress, Amélioration de la majoration de $g(4)$ dans le problème de Waring: $g(4) < 30$	137
Koji Katayama, On Ramanujan's formula for values of Riemann zeta-function at positive odd integers	149
Bohuslav Diviš, On the sums of continued fractions	157
Yoichi Motohashi, On the distribution of the divisor function in arithmetic progressions	175
P. Erdős and R. E. Hall, On the values of Euler's $\varphi$ -function	201
William A. Webb, Waring's problem in $\mathbb{G}F[q, \varepsilon]$	207
A. Schinzel, On a theorem of Bauer and some of its applications II	221
Б. В. Левин, А. А. Юдин, Локальные предельные теоремы для аддитивных арифметических функций	233

La revue est consacrée à la Théorie des Nombres  
 The journal publishes papers on the Theory of Numbers  
 Die Zeitschrift veröffentlicht Arbeiten aus der Zahlentheorie  
 Журнал посвящен теории чисел

L'adresse de la Rédaction et de l'échange	Address of the Editorial Board and of the exchange	Die Adresse der Schriftleitung und des Austausches	Адрес редакции и книгообмена
---	--	--	------------------------------

ACTA ARITHMETICA

ul. Śniadeckich 8, 00-950 Warszawa (Poland)

Les volumes IV et suivants sont à obtenir chez	Volumes from IV on are available at	Die Bände IV und folgende sind zu beziehen durch	Томы IV и следующие можно получить через
--	-------------------------------------	--	--

Ars Polona-Ruch, Krakowskie Przedmieście 7, 00-068 Warszawa (Poland)

Les volumes I-III sont à obtenir chez	Volumes I-III are available at	Die Bände I-III sind zu beziehen durch	Томы I-III можно получить через
---------------------------------------	--------------------------------	--	---------------------------------

Johnson Reprint Corporation, 111 Fifth Ave., New York, N. Y.

PRINTED IN POLAND

WROCLAWSKA DRUKARNIA NAUKOWA

## Exponents of the class groups of complex quadratic fields

by

P. J. WEINBERGER (Ann Arbor, Mich.)

1. Let  $-d$  be the discriminant of a complex quadratic field. Denote the class number of  $Q(\sqrt{-d})$  with  $h(-d)$ , and the exponent of the class group of  $Q(\sqrt{-d})$  with  $E(-d)$ . Then  $E(-d)$  is the smallest positive integer  $n$  such that  $\alpha^n$  is principal for all ideals  $\alpha$  of  $Q(\sqrt{-d})$ . Despite the importance of the class group in algebraic number theory, surprisingly little is known about its structure, even for complex quadratic fields, which, having regulator one, are the simplest fields to deal with. Heilbronn [5] showed that as  $d$  goes to infinity, so does  $h(-d)$ . I shall show that  $\lim E(-d) = \infty$ , but only by making strong and unproved assumptions about the zeros of  $L$ -functions. Upper bounds for the  $d$  such that  $h(-d) \leq 2$  are known ([2], [8]), and I shall give weaker results for  $E(-d) \leq 3$ .

Each discriminant  $-d$  factors uniquely into relatively prime elements of the set

$$-4, 8, -8, (-1)^{(p-1)/2} p, \quad \text{with } p \text{ an odd prime,}$$

of fundamental discriminants. If  $-d$  is the product of  $g$  fundamental discriminants, then it is well known that there are exactly  $2^{g-1}$  2-power groups in the decomposition of the class group of  $Q(\sqrt{-d})$  into cyclic groups of prime power order.

Let

$$\chi(n) = \chi_{-d}(n) = (-d|n)$$

be the Kronecker symbol. Throughout this paper I shall assume  $d > 4$ . Then if

$$L(s, \chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s} = \sum_{n=1}^{\infty} \frac{(-d|n)}{n^s}, \quad \text{Re}(s) > 0,$$

it is well known that

$$(1) \quad h(-d) = \sqrt{d} L(1, \chi) / \pi.$$



Some of the results in this paper depend on unproved hypotheses about the zeros of  $L(s, \chi)$  near  $s = 1$ . There are no zeros with  $\text{Re}(\sigma) \geq 1$ , and I shall denote by  $H(\varepsilon, -d)$  the statement that  $L(s, \chi) = 0$  implies  $|s - 1| > \varepsilon$  with  $\chi = \chi_{-d}$ .

LEMMA 1 ([6]). *Assuming  $H(\varepsilon, -d)$ , there is a constant  $c_1$ , depending only on  $\varepsilon$ , such that*

$$L(1, \chi) > \frac{c_1}{\log \log d \log \log \log d}.$$

The following two results, due to T. Tatzuzaawa [10], are not as strong as Lemma 1, but do not have any unverifiable hypotheses.

LEMMA 2. *If  $d \geq e^{1/\varepsilon}$ ,  $0 < \varepsilon < 1/2$ , and if  $L(1, \chi) \leq .655 \varepsilon d^{-\varepsilon}$ , then  $L(s, \chi)$  has a real zero  $s$ , with  $1 - \varepsilon/4 \leq s < 1$ .*

LEMMA 3. *There is at most one  $d$  with  $d \geq \text{Max}(e^{1/\varepsilon}, e^{11.2})$  and  $L(1, \chi) \leq .655 \varepsilon d^{-\varepsilon}$ .*

2.  $E(-d) = 2$  is equivalent to having one ideal class in each genus. Chowla [3] showed that this happens for only finitely many  $d$ . When  $d$  is even, the  $d/4$  with  $E(-d) = 2$  are essentially the idoneal numbers of Euler. If  $E(-d) = 2$  and  $-d$  is the product of  $g$  fundamental discriminants, then

$$(2) \quad h(-d) = 2^{g-1}$$

while

$$d \geq d_g = p_1 \cdot p_2 \cdot \dots \cdot p_g,$$

where  $p_n$  is the  $n$ th prime ( $p_1 = 2$ ). It is easy to see that if  $g \geq 11$ , then

$$d_g \geq d_{11} 37^{g-11} \geq 2 \cdot 10^{11} \cdot 37^{g-11}.$$

LEMMA 4. *If  $L(s, \chi) \neq 0$  in the interval  $1 - \frac{1}{4 \log d} \leq s < 1$  with  $d \geq d_{11}$ , then  $E(-d) > 2$  for all  $d \geq d_{11}$ .*

*Without any hypothesis, there is at most one  $d \geq d_{11}$  such that  $E(-d) = 2$ .*

*Proof.* Suppose that  $d \geq d_{11}$  and  $-d$  is the product of  $g$  fundamental discriminants.

To prove part one, Lemma 2 with  $\varepsilon = \frac{1}{\log d}$  gives

$$2^{g-1} = h(-d) > \frac{.655}{\pi e} \cdot \frac{\sqrt{d}}{\log d} \geq \frac{.655}{\pi e} \cdot \frac{\sqrt{d_{11}}}{\log d_{11}} > 1315,$$

so  $g > 11$ . Then Lemma 2 and the inequality for  $d_g$  give

$$2^{g-1} = h(-d) > \frac{.655}{\pi e} \cdot \frac{\sqrt{d_{11}} \cdot 37^{(g-11)/2}}{\log d_{11} + (g-11) \log 37} > \frac{.655}{\pi e} \cdot \frac{\sqrt{d_{11}} 6^{g-11}}{\log d_{11} + (g-11) \log 37},$$

so that

$$2^{20} > \frac{.655}{\pi e} \cdot \frac{\sqrt{d_{11}} 3^{g-11}}{\log d_{11} + (g-11) \log 37} > 1315,$$

since the middle term is an increasing function of  $g$ . This contradiction proves the first part of the Lemma.

To prove the second part, let  $\varepsilon = \frac{1}{\log d_{11}}$  in Lemma 3. Note that  $\log d_{11} > 26$ . Then, except for at most one  $d \geq d_{11}$ ,

$$2^{g-1} = h(-d) > \frac{.655}{\pi e} \cdot \frac{\sqrt{d_{11}}}{\log d_{11}} > 1315,$$

so again  $g > 11$ . Then

$$2^{g-1} = h(-d) > \frac{.655}{\pi e} \cdot \frac{\sqrt{d_{11}}}{\log d_{11}} \cdot 37^{(g-11) \left(\frac{1}{2} - \frac{1}{\log d_{11}}\right)},$$

so

$$2^{g-1} > \frac{.655}{\pi e} \cdot \frac{\sqrt{d_{11}}}{\log d_{11}} \cdot 2^{g-11} > 1315 \cdot 2^{g-11}. \text{ QED.}$$

**THEOREM 1.** *There is at most one complex quadratic field with  $d > 5460$  and  $E(-d) = 2$ . If  $L(s, \chi) \neq 0$  for  $d \geq d_{11} > 2 \cdot 10^{11}$  and  $1 - \frac{1}{4 \log d} \leq s < 1$ , then  $E(-d) = 2$  implies  $d \leq 5460$ .*

*Proof.* The theorem will follow from Lemma 4 when it is shown that  $E(-d) \neq 2$  for  $5460 < d < d_{11}$ . Each ideal class of  $Q(\sqrt{-d})$  contains an integral ideal with norm  $< \sqrt{d}/3$ . If  $(-d/p) = 1$ , then  $(p) = p\bar{p}$ . If  $p^2$  is principal, say  $p^2 = (a)$ , then  $p^2 = N(a) \geq d/4$ , so  $p > \sqrt{d}/4$ . Hence, if  $d > 79707$ ,  $\sqrt{d}/4 > 163$ , so for each  $p \leq 163$ ,  $E(-d) = 2$  implies  $(-d/p) \neq 1$ . Using his delay line sieve D. H. Lehmer has found there are no such  $d < d_{11}$ . The range  $5460 < d \leq 79707$  contains no  $d$  with  $E(-d) = 2$ , as J. D. Swift [9] showed. QED.

This theorem is an improvement on the results of Briggs and Chowla [4].

3. LEMMA 5. Let  $\mathfrak{a}$  be an integral ideal of  $Q(\sqrt{-d})$  and  $c$  a positive integer such that  $\mathfrak{a}^c$  is principal. If  $\mathfrak{a}$  is not a principal ideal generated by a rational integer, and if  $\mathfrak{a}$  is prime to  $d$ , then  $(N\mathfrak{a})^c > d/4$ .

Proof. Suppose  $\mathfrak{a}^c = (a)$  where  $a$  is a rational integer. Then in  $Q(\sqrt{-d})$

$$(3) \quad (a) = \prod p_i^{2n_i} \prod (q_i \bar{q}_i)^{m_i} \prod (r_i)^{l_i}$$

where the  $p_i, q_i, (r_i)$  are ramified, completely split, and inert primes of  $Q(\sqrt{-d})$ , respectively. But the  $r_i$  are all 0 since  $a$  is prime to  $d$ , and, by hypothesis, all the  $m_i$  and  $l_i$  are divisible by  $c$ . This implies that  $a$  is generated by a rational integer, which is a contradiction, so  $\mathfrak{a}$  is not rational, so  $(N\mathfrak{a})^c = Na > d/4$ . QED.

The next theorem proves a conjecture of D. Shanks [7].

THEOREM 2. There are only finitely many complex quadratic fields with  $E(-d) = 3$ .

Proof. Suppose  $E(-d) = 3$ , and let  $p$  be the smallest rational prime with  $(-d|p) = 1$ . Then  $(p) = \mathfrak{p}\bar{\mathfrak{p}}$ , and  $\mathfrak{p}$  is not a principal ideal generated by a rational integer. Lemma 5 implies that  $\mathfrak{p}^3 = (N\mathfrak{p})^3 > d/4$ . But for large enough  $d$  this contradicts the result of A. I. Vinogradov and Ju. V. Linnik [11] that  $p \ll d^{1/4+\epsilon}$ . QED.

4. LEMMA 6. Let  $a$  be a positive rational integer with the prime decomposition (3). Then the number of distinct integral ideals of  $Q(\sqrt{-d})$  with norm  $a$  and no non-trivial principal ideal factors is at most

0 if an  $l_i > 0$  or an  $n_i > 1$ , and  
 $2^{M_a}$  if all  $l_i = 0$  and all  $n_i \leq 1$ , where  $M_a$  is the number of non-zero  $m_i$  in (3).

Proof. From (3) it follows that if  $a = N\mathfrak{b} = \mathfrak{b}\bar{\mathfrak{b}}$ , then each  $l_i$  is even and

$$\mathfrak{b} = \prod p_i^{n_i} \prod q_i^{j_i} \bar{q}_i^{m_i - j_i} \prod (r_i)^{l_i/2}$$

where  $0 \leq j_i \leq m_i$ . If any  $l_i > 0$ , then  $(r_i)|\mathfrak{b}$  so all  $l_i = 0$ . If  $1 < j_i < m_i$ , then  $(q_i)|\mathfrak{b}$ , so each of the  $M_a$  numbers  $j_i$  may be 0 or  $m_i$ . If some  $n_i \geq 2$ , then  $(p_i)|\mathfrak{b}$ . QED.

LEMMA 7. If  $\omega(n)$  is the number of distinct prime factors of  $n$ , then

$$\sum_{\substack{n \leq x \\ p|n \Rightarrow p \geq y}} 2^{\omega(n)} \ll \frac{x \log x}{\log^2 y},$$

where the implied constant is absolute.

Proof.

$$\begin{aligned} \sum_{\substack{n \leq x \\ p|n \Rightarrow p \geq y}} 2^{\omega(n)} &= \sum_{\substack{n \leq x \\ p|n \Rightarrow p \geq y}} \sum_{d|n} \mu^2(d) \\ &= \sum_{\substack{d \leq x \\ p|d \Rightarrow p \geq y}} \mu^2(d) \sum_{\substack{k \leq \frac{x}{d} \\ p|k \Rightarrow p \geq y}} 1 \ll \sum_{\substack{d \leq x \\ p|d \Rightarrow p \geq y}} \mu^2(d) \frac{x}{d} \cdot \frac{1}{\log y} \end{aligned}$$

since

$$\sum_{\substack{n \leq x \\ p|n \Rightarrow p \geq y}} 1 \ll \frac{x}{\log y}.$$

Hence the sum of the Lemma is

$$\ll \frac{x}{\log y} \sum_{\substack{d \leq x, p|d \Rightarrow p \geq y \\ d \text{ squarefree}}} \frac{1}{d} \ll \frac{x}{\log y} \prod_{y < p \leq x} \left(1 + \frac{1}{p}\right) \ll \frac{x}{\log y} \cdot \frac{\log x}{\log y},$$

since

$$\log n \ll \prod_{p \leq n} \left(1 + \frac{1}{p}\right) \ll \log n. \text{ QED.}$$

Let  $-d = \prod_{i=1}^g d_i$ , where the  $d_i$  are fundamental discriminants, and let  $p_i$  be the unique rational prime dividing  $d_i$ .

LEMMA 8. With the above notation, if  $(-d|p) = 1$  for a prime  $p$  implies that  $p > y$ , then

$$h(-d) \ll \frac{\sqrt{d} \log d \log(g+1)}{\log^2 y},$$

where the implied constant is absolute.

Proof. During this proof, adopt the convention that  $2^{\omega(x)} = 0$  if  $x$  is not an integer. Let  $b(\mathfrak{a})$  denote the number of integral ideals  $\mathfrak{a}$  with norm  $a$ , such that  $\mathfrak{a}$  is the integral ideal of smallest norm in its ideal class. Such an  $\mathfrak{a}$  can have no non-trivial principal divisors, so that  $b(\mathfrak{a})$  is at most the number of Lemma 6. Since every ideal class contains an ideal with norm less than  $\sqrt{d}/3$ ,

$$h(-d) \leq \sum_{n \leq \sqrt{d}/3} b(n).$$

Let

$$\begin{aligned} s(\mathfrak{a}) = \left\{ n \leq \sqrt{d}/3 : n = \prod_{i=1}^g p_i^{a_i} \prod_{i=1}^{M_n} q_i^{b_i}, \text{ with } a_i = 0 \text{ or } 1, \right. \\ \left. b_i > 0, (-d|q_i) = 1, \text{ and } \sum_{i=1}^g a_i = a \right\}. \end{aligned}$$

Let  $s = \bigcup_{a=0}^g s(a)$ . Then by Lemma 6,

$$\begin{aligned} h(-d) &\leq \sum_{n \in s} 2^{2M_n} = \sum_{n \in s(0)} 2^{\omega(n)} + \sum_{i=1}^g \sum_{n \in s(i)} 2^{\omega(n/p_i)} + \\ &\quad + \sum_{1 \leq i < j \leq g} \sum_{n \in s(i,j)} 2^{\omega(n/p_i p_j)} + \dots + \sum_{n \in s(g)} 2^{\omega(n/p_1 \dots p_g)} \\ &\ll \frac{\sqrt{d} \log d}{\log^2 y} \left( 1 + \sum_{i=1}^g \frac{1}{p_i} + \sum_{1 \leq i < j \leq g} \frac{1}{p_i p_j} + \dots + \frac{1}{p_1 \dots p_g} \right) \\ &= \frac{\sqrt{d} \log d}{\log^2 y} \prod_{i=1}^g \left( 1 + \frac{1}{p_i} \right) \ll \frac{\sqrt{d} \log d \log(g+1)}{\log^2 y}, \end{aligned}$$

by Lemma 7, and since  $\prod_{i=1}^g \left( 1 + \frac{1}{p_i} \right) \ll \log(g+1)$ . QED.

**THEOREM 3.** *If there is an  $\varepsilon > 0$  such that  $H(\varepsilon, -d)$  is true for all sufficiently large  $d$ , then*

$$E(-d) > \frac{c_3(\varepsilon)}{\log \log d} \left( \frac{\log d}{\log \log \log d} \right)^{1/2}.$$

*Proof.* Let  $p$  be the smallest prime such that  $(-d|p) = 1$ . Let  $(p) = p\bar{p}$ . If  $p$  is principal, Lemma 5 gives  $p = N\bar{p} > d/4$  which contradicts, for large enough  $d$ , the result of Vinogradov and Linnik quoted in Theorem 2. If  $p$  is not principal Lemma 5 gives

$$p^{E(-d)} > d/4.$$

In Lemma 8 take  $y = (d/4)^{1/E(-d)}$ , so

$$h(-d) \ll \frac{\sqrt{d}}{\log d} E(-d)^2 \log(g+1) \ll \frac{\sqrt{d} E(-d)^2}{\log d} \log \log d,$$

since  $d \geq \prod_{i=1}^g p_i$  implies  $g \ll \log d$ . On the other hand Lemma 1 gives

$$h(-d) \geq \frac{c_1(\varepsilon) \sqrt{d}}{\log \log d \log \log \log d}.$$

Combining the two estimates for  $h(-d)$  gives the conclusion. QED.

5. It is of some interest to see how the conclusion of Theorem 3 changes when the hypothesis is modified.

**THEOREM 4.** *If  $L(s, \chi) \neq 0$  for  $\text{Re}(s) > 1/2$ , then*

$$E(-d) \geq \log d / \log \log d$$

for fundamental discriminants  $-d$ .

*Proof.* The argument of N. Ankeny [1] shows that the smallest prime  $p$  with  $(-d|p) = 1$  satisfies  $p \ll (\log d)^2$ . Hence  $(\log d)^{2E(-d)} \geq d/4$ . QED.

Finally, the hypothesis of Theorem 3 is not the weakest under which it is easy to see that  $E(-d) \rightarrow \infty$  as  $d \rightarrow \infty$ . An easy modification of Landau's proof of Lemma 1 shows that

$$H\left(\frac{(\log \log d)^{2+\varepsilon}}{\log d}, -d\right)$$

implies

$$L(1, \chi) \geq \frac{c_3(\varepsilon) (\log \log d)^{1+\varepsilon}}{\log d},$$

from which the proof of Theorem 3 shows that  $E(-d)$  is not bounded.

Notes added in proof:

1. Boyd and Kisilevsky (Proc. AMS 31 (1972)) also prove Theorems 2 and 4.
2. Montgomery (to appear) has recently shown that if  $L(s, \chi) \neq 0$  when  $\sigma > 1 - \delta$ ,  $|t| \leq \delta^2 \log d$ , for some  $\delta \leq 1/2$ , then there is a prime  $p$  with  $(-d|p) = 1$  and  $p^\delta \ll \delta \log d$ . With this hypothesis,

$$E(-d) \geq \frac{\delta \log d}{\log(\delta \log d)},$$

which is Theorem 4 when  $\delta = 1/2$ . Further, if  $f(d) \rightarrow \infty$  and if  $H(f(d)/\log d, -d)$  holds for all large  $d$ , then  $E(-d) \rightarrow \infty$ .

#### References

- [1] N. Ankeny, *The least quadratic non residue*, Annals of Math. 55 (1952), pp. 65-72.
- [2] A. Baker and H. Stark, Annals of Math. 94(1971).
- [3] S. Chowla, *An extension of Heilbronn's class-number theorem*, Quart. J. Math. Oxford 2, 5 (1934), pp. 304-307.
- [4] S. Chowla and W. Briggs, *On discriminants of binary quadratic forms with a single class in each genus*, Canad. J. Math. 6 (1954), pp. 463-470.
- [5] H. Heilbronn, *On the class-number in imaginary quadratic fields*, Quart. J. Math. Oxford 2, 5 (1934), pp. 150-160.
- [6] E. Landau, *Über die Wurzeln der Zeta Funktion eines algebraischen Zahlkörpers*, Math. Ann. 79 (1919), pp. 388-401.
- [7] D. Shanks, J. Num. Theory (to appear).
- [8] H. Stark, *A complete determination of the complex quadratic fields of class number one*, Mich. Math. Journ. 14 (1967), pp. 1-27.

- [9] J. D. Swift, *Note on discriminants of binary quadratic forms with one class in each genus*, Bull. AMS 54 (1948), pp. 560-561.  
 [10] T. Tatzuza, *On a theorem of Siegel*, Japan. J. Math. 21 (1951), pp. 163-178.  
 [11] A. I. Vinogradov and Ju. V. Linnik, *Hyperelliptic curves and the least prime quadratic residue*, Soviet Math. (Doklady) (1966), pp. 612-614.

Received on 5. 6. 1971

(177)

## A remark on Hilbert's Theorem 92

by

DONALD L. MCQUILLAN (Madison, Wisc.)

Let  $K$  be an algebraic number field and  $G$  a cyclic group of automorphisms of  $K$  of odd prime order  $p$ . Let  $U$  denote the units of  $K$ . Then Hilbert's Theorem 92 states that  $H^1(G, U)$  is not trivial; however Hilbert's Zahlbericht [3] does not contain a precise expression for the order of the group. In Hasse's Zahlbericht [2] the following expression, due to Takagi, is given:

$$|H^1(G, U)| = p^{r+1-q+t}.$$

Here  $r$  ( $= r_1 + r_2 - 1$  with the usual notation) is the rank of  $U$ ,  $t$  is 1 if  $K$  contains a primitive  $p$ th root of unity and is 0 otherwise, and  $q$  is defined by the equation  $[N(U): U_0^p] = p^q$  where  $N$  is the norm from  $K$  to  $K^G$  and  $U_0$  is the group of units of  $K^G$ .

The purpose of this short note is to derive another, quite different, expression for the order of  $H^1(G, U)$  which does not seem to have appeared in the literature before. At the end we give a result on  $H^1(G, \theta)$  where  $\theta$  is the maximal order in  $K$ . We need some notation. Let  $u_1, u_2, \dots, u_r$  be a set of free generators of  $U$  and let  $\sigma$  be a generator of  $G$ . Then  $\sigma u_i = \zeta_i u_1^{\alpha_{i1}} u_2^{\alpha_{i2}} \dots u_r^{\alpha_{ir}}$  where  $\zeta_i$  is a root of unity and  $\alpha_{i1}, \alpha_{i2}, \dots, \alpha_{ir}$  are rational integers,  $1 \leq i \leq r$ . The integral  $r \times r$  matrix  $A = (a_{ij})$  has period  $p$  and so there exists [4] a unimodular matrix  $V$  such that

$$VAV^{-1} = \text{diag}\{I_a, B_1, \dots, B_b, S_1, \dots, S_c\}$$

where  $I_a$  is the  $a \times a$  identity matrix,  $B_1, \dots, B_b$  are  $(p-1) \times (p-1)$  indecomposable matrices, and  $S_1, \dots, S_c$  are  $p \times p$  indecomposable matrices. The integers  $a, b, c$  depend only on  $U$ . We shall prove

**THEOREM.** *The order of  $H^1(G, U)$  is  $p^{a+1+\varepsilon}$  where  $\varepsilon = 0, 1$  or  $-1$ . If  $K$  contains no primitive  $p$ -th root of unity then  $\varepsilon = 0$ ; if  $a = 0$  then  $\varepsilon = 0$  or  $1$ .*

**Proof.** Let  $U_1$  denote the group of roots of unity in  $K$ . Then  $G$  acts on  $U_1$ , and it follows at once that the order of  $H^r(G, U_1)$ ,  $r \in \mathbb{Z}$ , is  $p^t$  where  $t$  has the meaning assigned above. Next,  $U/U_1$  is free on  $r$  generators,  $G$  acts