[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. Tatuzawa, *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)

ACTA ARITHMETICA
XXII (1973)

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 pth 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 θ is the maximal order in K. We need some notation. Let $u_1, u_2, \ldots, u_r$ be a set of free generators of U and let σ be a generator of G. Then $\sigma u_i = \zeta_i u_1^{a_{i1}} u_2^{a_{i2}} \ldots u_r^{a_{ir}}$ where ζ_i is a root of unity and $a_{i1}, a_{i2}, \ldots, a_{ir}$ are rational integers, $1 \leqslant i \leqslant r$. The integral $r\times r$ matrix $A = (a_{ij})$ has period p and so there exists [4] a unimodular matrix V such that

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

where I_a is the $a\times a$ identity matrix, $B_1, \ldots, B_b$ are $(p-1)\times(p-1)$ indecomposable matrices, and $S_1, \ldots, S_c$ 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 $H^r(G, U_1)$, $r \in Z$, is p^t where t has the meaning assigned above. Next, U/U_1 is free on r generators, G acts on this group, and from our remarks above we can choose a basis $v_1, v_2, \ldots, v_r$ of U/U_1 such that $\sigma v_i = v_1^{a_{i1}} \ldots v_r^{a_{ir}}, 1 \leq i \leq r$, where $A = (a_{ij})$ has the diagonal form given previously. We compute $H^r(G, U/U_1)$ as follows. The contribution of each component in the diagonal matrix $A = \mathrm{diag}\{I_a, B_1, \ldots, B_b, S_1, \ldots, S_c\}$ can be computed separately, in fact, with an obvious notation

$$H^r(G, U/U_1) \cong H^r(I_a, Z^a) \oplus H^r(B_1, Z^{p-1}) \oplus \ldots \oplus H^r(S_c, Z^p).$$

Clearly $H^0(I_a, Z^a) \cong Z_p^a$ and $H^1(I_a, Z^a) \cong (0)$ where $Z_p = Z/pZ$. Let $B = B_i, 1 \leqslant i \leqslant b$. Now the characteristic roots of B are the primitive pth roots of unity so that $\sum_{i=0}^{p-1} B^i = 0$, and the Smith normal form of $B - I$ is $\mathrm{diag}\{p, 1, \ldots, 1\}$. We can conclude at once that

$$H^0(B, Z^{p-1}) = (0), \quad H^1(B, Z^{p-1}) \cong Z_p.$$

Let $S = S_j, 1 \leqslant j \leqslant c$. Since $S = \begin{pmatrix} B & 0 \\ x & 1 \end{pmatrix}$ where B is an indecomposable $(p-1) \times (p-1)$ matrix and $x \in Z^{p-1}$ we can conclude (see for instance [1]) that

$$\sum_{i=0}^{p-1} S^i = \begin{pmatrix} 0 \\ z \end{pmatrix}$$

where $z = (z_1, \ldots, z_p) \in Z^p$ and $z_1, \ldots, z_p$ are relatively prime. Furthermore if $y = (y_1, \ldots, y_p) \in Z^p$ then $(S - I)y^t = 0$ if and only if $y_1 = \ldots = y_{p-1} = 0$. Finally the Smith normal form of $S - I$ is $(0, 1, \ldots, 1)$. From these facts it is immediate that

$$H^0(S, Z^p) = H^1(S, Z^p) = (0).$$

Adding up all contributions we get

$$H^0(G, U/U_1) \cong Z_p^a, \quad H^1(G, U/U_1) \cong Z_p^b.$$

Now $a + (p-1)b + pc = r = r_1 + r_2 - 1$; furthermore since $a + c$ is the multiplicity of the characteristic root 1 in A we get $a + c = R = R_1 + R_2 - 1$ where R is the rank of the units U_0 in K^G and R_1, R_2 have the usual meanings. Since p is odd we get $r_i = pR_i, i = 1, 2$. From these relations we see that $b = a + 1$.

From the exact sequence of G-modules

$$1 \to U_1 \to U \to U/U_1 \to 1,$$

we get the exact sequence of Tate groups (taking into account the values obtained above for cohomology groups of U_1 and U/U_1)

$$\to Z_p^a \xrightarrow{\alpha} Z_p^t \xrightarrow{\beta} H^1(G, U) \xrightarrow{\gamma} Z_p^b \xrightarrow{\delta} Z_p^t \to \ldots$$

A straightforward calculation shows then that $H^1(G, U) \cong Z_p^{b+\varepsilon} = Z_p^{a+1+\varepsilon}$ where $\varepsilon = 0, 1$ or -1. However if both β and δ are trivial (in particular if $t = 0$) we get $H^1(G, U) \cong Z_p^b = Z_p^{a+1}$. Finally, suppose $a = 0$. If also $t = 0$ then we have just seen that $H^1(G, U) \cong Z_p$. However if $t \neq 0$ then β is a monomorphism and so $H^1(G, U)$ is not trivial, i.e. $\varepsilon = 0$ or 1. This completes the proof of the theorem.

Consider now the group $H^1(G, \theta)$ where θ is the maximal order in K. If $[K:\boldsymbol{Q}] = N$ and $w_1, w_2, \ldots, w_N$ is Z-integral basis for θ then we can write

$$\sigma w_i = \sum_{j=1}^{N} a_{ij} w_j, \quad 1 \leqslant i \leqslant N,$$

where $a_{ij} \in Z$ and the matrix $A = (a_{ij})$ has period p. As above we can assume $A = \mathrm{diag}\{I_u, B_1, \ldots, B_v, S_1, \ldots, S_w\}$ and the previous calculations show that

$$H^0(G, \theta) \cong Z_p^u, \quad H^1(G, \theta) \cong Z_p^v.$$

Now $u + (p-1)v + pw = [K: \boldsymbol{Q}] = N$, $u + w = [K^G: \boldsymbol{Q}] = N/p$ and from these relations we can conclude that $u = v$. We therefore have another proof of the well-known fact (cf. [5], [6]) that $H^1(G, \theta) \cong H^0(G, \theta)$ in this case. Finally, we would like to write down explicit values for u, v, w. Our relations above give $v = u$ and $w = [K^G: \boldsymbol{Q}] - u$. However $H^0(\boldsymbol{Q}, \theta) \cong \theta^G/T_G(\theta)$ where θ^G are the elements of θ fixed by G, i.e. θ^G = the maximal order in K^G, and T_G is the trace from K to K^G. Let $\mathfrak{p}$ be a prime ideal of θ^G. Put $E(\mathfrak{p})$ = the ramification index of $\mathfrak{p}$ over Z, $F(\mathfrak{p})$ = the relative degree of $\mathfrak{p}$ over Z, $e(\mathfrak{p})$ = the ramification index of $\mathfrak{p}$ in θ, $m(\mathfrak{p})$ = the differential exponent of any prime ideal of θ over $\mathfrak{p}$. Now $T_G(\theta) = \prod_{\mathfrak{p}} \mathfrak{p}^{[m(\mathfrak{p})/e(\mathfrak{p})]}$ where the product runs through all prime ideals of θ^G and $[x]$ is the largest integer in x. It follows that

$$|H^0(G, \theta)| = |\theta^G/T_G(\theta)| = p^{\sum_{\mathfrak{p}} F(\mathfrak{p})[m(\mathfrak{p})/e(\mathfrak{p})]}$$

and so $u = \sum_{\mathfrak{p}} F(\mathfrak{p})\,[m(\mathfrak{p})/e(\mathfrak{p})]$. It is clear that $m(\mathfrak{p}) = e(\mathfrak{p}) - 1$ unless $\mathfrak{p}$ divides p in θ^G. Bearing in mind that $[K^G: \boldsymbol{Q}] = \sum_{\mathfrak{p}|p} E(\mathfrak{p})F(\mathfrak{p})$ we get

THEOREM. *With the preceding notations we have*

$$v = u = \sum_{\mathfrak{p}|p} F(\mathfrak{p})\,[m(\mathfrak{p})/e(\mathfrak{p})],$$

$$w = \sum_{\mathfrak{p}|p} F(\mathfrak{p})\{E(\mathfrak{p}) - [m(\mathfrak{p})/e(\mathfrak{p})]\},$$

where the summation is over the primes $\mathfrak{p}$ of θ^G which divide p.

Bibliography

[1] W. B. Giles and D. L. McQuillan, *A problem on rational invariants*, J. Number Theory 1 (1969), pp. 375–384.

[2] H. Hasse, *Bericht über neuere Untersuchungen und Probleme aus der Theorie der algebraischen Zahlkörper*, 3 Auflage, Wurzburg–Wien 1970.

[3] D. Hilbert, *Gesammelte Abhandlungen*, erster Band, *Zahlentheorie*, Berlin 1932.

[4] I. Reiner, *Integral representations of cyclic groups of prime order*, Proc. Amer. Math. Soc. 8 (1957), pp. 142–146.

[5] M. Rosen, *Two theorems on Galois cohomology*, Proc. Amer. Math. Soc. 17 (1966), pp. 1183–1185.

[6] H. Yokoi, *A note on the Galois cohomology group of the ring of integers in an algebraic number field*, Proc. Japan Acad. 40 (1964), pp. 245–246.

Received on 12. 8. 1971 (204)

ACTA ARITHMETICA
XXII (1973)

Asymptotisches Verhalten einer diophantischen Approximations-Funktion

von

R. Schark und J. M. Wills (Berlin)

R sei die Menge der reellen Zahlen; N der natürlichen, Z der ganzen, $F = R - Z$ der nichtganzen Zahlen. Zu einem $x \in R$ sei $\|x\|$ der Abstand von der nächsten ganzen Zahl und $[x]$ die größte ganze Zahl $\leqslant x$. Weiter sei $n \in N$, $\alpha = (\alpha_1, \ldots, \alpha_n) \in F^n$ und

$$\omega(n) = \inf_{\alpha \in F^n} \sup_{q \in Z} \min_{1 \leqslant i \leqslant n} \|q\alpha_i\|.$$

In der vorliegenden Arbeit wird das asymptotische Verhalten von $\omega(n)$ untersucht. Zuvor seien die bisherigen Ergebnisse über $\omega(n)$ zusammengestellt:

Zu einem $z \geqslant 2$, $z \in N$ sei $z = \prod_{i=1}^{h} p_i^{c_i}$ die kanonische Primzahlzerlegung und $h(z) = h$ bei nichtprimem z die Anzahl der verschiedenen Primteiler von z und $h(z) = h = 0$, wenn z prim ist. Weiter sei $\|x\|_z = \min_{g \in Z} |x - gz|$. Dann ist nach [5], S. 170:

$$(1) \qquad \omega(n) = \inf_{a,z} \left\{ \frac{a}{z} \,\middle|\, a \in N, z \in N, h(z) \leqslant n;\ \text{es gibt ein } k = (k_1, \ldots, k_n) \in N^n \text{ mit } 0 < k_i < z, 1 \leqslant i \leqslant n \text{ und } \max_{1 \leqslant q \leqslant z} \min_{1 \leqslant i \leqslant n} \|qk_i\|_z \leqslant a \right\}.$$

Nach [3], Lemma 2, ist $\omega(1) = \frac{1}{3}$ und nach [4], Satz 2:

$$\frac{1}{2n^2} \leqslant \omega(n) \leqslant \frac{1}{w(n)} \quad \text{für} \quad n \geqslant 2.$$

Dabei ist $w(n) = \max\{z \mid \frac{1}{2}\varphi(z) + h(z) \leqslant n\}$, φ die Euler-Funktion. Nach [4], Satz 1, ist $w(1) = 3$, $w(2) = 5$, $w(3) = 8$ und

$$6(n-2) \leqslant w(n) \leqslant n^2 - 4 \quad \text{für} \quad n \geqslant 4.$$

Cusick zeigte in [1]:

$$\omega(n) = \frac{1}{w(n)} \text{ für } n = 2, \ldots, 7 \quad \text{und} \quad w(n) = 6(n-2) \text{ für } n = 4, \ldots, 7.$$

Vermutlich gilt $\omega(n) = 1/w(n)$ für alle $n \geqslant 1$.