ON THE UNITS OF AN ALGEBRAIC NUMBER FIELD

BY

JAMES AX[1]

Introduction

Let K be an algebraic number field of degree n over the field of rational numbers Q. Let p be a rational prime and denote the p-adic completion of Q by Q_p. Let A denote the completion of the algebraic closure of Q_p equipped with its valuation $| \ |_p$ normed so that $| p |_p = 1/p$. Let T be the set of n distinct monomorphisms of K into A.

The p-adic rank $r_p = r_{K,p}$ of the units U of K is defined as the rank of the p-adic regulator matrix

$$\mathcal{R}_p = (\log_p \tau(V_i))_{\tau \in T, i=1,\cdots,r}$$

where $v_1, \cdots, v_r$ is a basis for a free direct summand of U of maximal rank ($r = r_K =$ dirichlet number of K) and where the p-adic logarithm is defined by the usual series for principal units and extended to all units of A by means of the functional equation. Thus if $v \in A$ is such that $| v - 1 |_p < 1$ then $\log_p v = -\sum_{k=1}^{\infty} (1 - v)^k/k \in A$ and if $| v |_p = 1$ then

$$\log_p v = (\log v^m)/m$$

for any positive integer m such that $| v^m - 1 |_p < 1$.

We have $r_p \leq r$. In the abelian case Leopoldt in [6] has raised the question of determining r_p and in particular asked if $r_{K,p} = r_K$ for all abelian K and rational primes p. In §1 we prove the following partial result on Leopoldt's problem.

THEOREM 1. *If K/Q is an abelian extension with galois group G of exponent m such that $m \leq 4$ or $m = 6$, then $r_p = r$.*

The proof uses Mahler's p-adic analogue [7], [8] of Hilbert's seventh problem (α^β is transcendental if α and β are algebraic numbers such that $\alpha \neq 0, 1$ and β is irrational). The same proof actually proves a slightly stronger result (Theorem 1′) as well as the following fact.

THEOREM 2. *If K/Q is normal and $r \geq 2$ then $r_p \geq 2$.*

In §2 an algebraic method is employed to solve the following special cases of Leopoldt's problem.

THEOREM 3. *Let p be a regular prime, let a be a positive integer, let ζ be a primitive p^a-th root of unity and let $K = Q(\zeta)$. We then have $r_p = r$.*

Received February 17, 1964.

[1] Work partially supported by the National Science Foundation.

The proof is an application of the main properties of the (absolute) Hilbert Class Field of K.

We remark that these results provide some instances for which Leopoldt's p-adic class formula $(3.2)_p$ of [6] does not reduce to $0 = 0$. At the close of §1, a conjecture generalizing Hilbert's seventh problem, which would completely solve Leopoldt's problem is noted.

We shall retain the above notation. In addition, Z = rational integers, Z_p = closure of Z in Q_p. We shall also find it convenient to introduce the (usually infinite) matrix.

$$R_p = (\log_p \tau(u))_{\tau \in T, u \in U_p}$$

where U_p = the group of units u such that $|\tau(u) - 1|_p < 1$ for all $\tau \in T$. Indeed for the relatively crude question of rank we are considering we can replace $\mathcal{R}_p$ by R_p since there exists a positive integer m such that $U^m \subseteq U_p$ which entails

$$r_p = \operatorname{rank} R_p .$$

1. A transcendental method

LEMMA. *Let H be an abelian group of automorphisms of an algebraic number field K, H_0 its character group ($x \in H_0$ may be assumed to take values in A). Let S be a subset of H and $\theta \in T$. If the α_s for $s \in S$ are such that*

$$\textstyle\sum_{h \in S} \alpha_h \log_p \theta(hu) = 0 \qquad \textit{for all } u \in U_p$$

then $(\alpha_h)_{h \in S}$ is an A-linear combination of the $(x(h))_{h \in S}$ for those $x \in H_0$ such that

$$\textstyle\sum_{h \in H} x(h) \log_p \theta(hu) = 0 \qquad \textit{for all } u \in U_p .$$

Proof. If $\tau \in T$ we define $L_\tau : U_p \to A$ by $L_\tau(u) = \log_p \tau u$ for all $u \in U_p$. We define W to be the A-vector space of functions from U_p to A. W has the structure of a (left) $A[H]$-module if we let hF for $h \in H$ and $F \in W$ be defined by

$$(hF)(u) = F(hu) \qquad \text{for all } u \in U_p ,$$

since H is abelian. Now suppose $\alpha_h \in A$ for $h \in H$ are such that

$$\textstyle\sum_{h \in H} \alpha_h \log_p \theta(hu) = 0 \qquad \text{for } u \in U_p , \tag{1}$$

which may be rewritten as

$$\textstyle\sum_{h \in H} \alpha_h\, h \cdot L_\theta = 0 \quad \text{in} \quad W.$$

Since H is abelian we have for all $g \in H$,

$$0 = g \textstyle\sum_{h \in H} \alpha_h\, h \cdot L_\theta = \sum_{h \in H} \alpha_h\, h \cdot gL_\theta . \tag{2}$$

Now $A[H]L_\theta$ is a cyclic $A[H]$-submodule of W and so there exists a unique ideal B of $A[H]$ which is $A[H]$-isomorphic to $A[H]L_\theta$ (as left $A[H]$-modules).

Equation (2) shows

$$\sum_{h\epsilon H} \alpha_h\, h\cdot B = 0.$$

Let V be the ideal of $A[H]$ such that $A[H] = V \oplus B$ as rings. We see that for vectors $(\alpha_h)_{h\epsilon H}$ with entries in A, (1) is equivalent to $\sum_{h\epsilon H} \alpha_h\, h \,\epsilon\, V$.

Since V has an A-basis consisting of $\sum_{h\epsilon H} x(h)h$ for certain $x \,\epsilon\, H_0$ as follows from (33.8) of [3], the lemma follows upon restriction to S.

Theorem 1 is contained in the following result.

THEOREM 1′. *If the maximal real subfield of a normal extension K/Q is an abelian extension of Q with galois group G of exponent m such that $m \leq 4$ or $m = 6$, then $r_p = r$.*

Proof. It suffices to consider the case where K/Q is a real abelian extension. Assume $m \leq 4$ or $m = 6$ and that $r_p < r = n - 1$. Thus the A-space of $(\alpha_g)_{y\epsilon G}$ with $\alpha_g \,\epsilon\, A$ such that

$$\sum_{g\epsilon G} \alpha_g \log_p \theta(gu) = 0 \qquad \text{for all } u \,\epsilon\, U_p$$

where θ is some element of T has dimension ≥ 2 since the matrix

$$R_p = (\log_p \theta(gu))_{g\epsilon G, u\epsilon U_p}$$

has rank $r_p \leq n - 2$. It follows from the lemma with $H = G$ that there are at least 2 different $x \,\epsilon\, G_0$, the character group of G, such that

$$(3) \qquad \sum_{g\epsilon G} x(g) \log_p \theta(gu) = 0 \qquad \text{for } u \,\epsilon\, U_p\,.$$

Let x be a non-principal character satisfying (3) and let E be the subfield of A generated over Q by the values $x(g)$, $g \,\epsilon\, G$. By our assumptions on m, $E = Q$ or $E =$ quadratic extension of Q. In any case we may assume x takes its values in a quadratic extension F/Q. Let $1, \delta$ be an integral basis of F. Then we may write

$$(4) \qquad x(g) - 1 = a(g) + b(g)\delta$$

where $a(g), b(g) \,\epsilon\, Z$ for $g \,\epsilon\, G$. This yields the relation

$$\sum_{g\epsilon G-1} (a(g) + b(g)\delta) \log_p \theta(gu) = 0 \qquad \text{for } u \,\epsilon\, U_p$$

which we may rewrite as

$$(5) \qquad \log_p \theta(\textstyle\prod_{g\epsilon G-1} gu^{a(g)}) = -\delta \log_p \theta(\textstyle\prod_{g\epsilon G-1} gu^{b(g)}).$$

By a theorem of Minkowski [9] (or [1]) there exists a unit v in U such that $\prod_{g\epsilon G-1} gv^{c(g)} =$ root of unity with each $c(g) \,\epsilon\, Z$ implies $c(g) = 0$ for $g \,\epsilon\, G - 1$. If $w = v^{N-1}$ where N is the number of elements in the residue class field of the prime of K above p, then w has the same property as v and $w \,\epsilon\, U_p$. Since x is not principal, it follows from (4) that some $a(g)$ or some $b(g)$ is not zero for some $g \,\epsilon\, G - 1$. It follows that at least one side, and hence both sides, of (5) are non-zero for $u = w$ because the p-adic logarithm is zero only for roots of unity (page 200 of [4]). (5) then implies that there exist two algebraic numbers in A such that the ratio of their p-adic logarithms is algebraic but irrational. This contradiction to the Mahler's theorem [7], [8] establishes Theorem 1′. A proof of Theorem 2 differs from this proof by a transposition. We first use Minkowski's theorem to find a $w \in U_p$ and an automorphism g of K such that if $w^c g w^d$ is a root of unity with $c, d \in Z$, then $c = d = 0$. We then apply the lemma with $H =$ group of automorphisms generated by g and with $S = \{1, g\}$. If $r_p < 2$ then the lemma yields a non-principal character x of H such that

$$\log_p \theta(u) + x(g) \log_p \theta(gu) = 0 \qquad \text{for } u \in U_p .$$

For $u = w$ this gives a contradiction to Mahler's theorem as before since $x(g)$ must be irrational by our choice of w.

Conjecture. Let B be either the field A as above or the field C of complex numbers. Let Q' be the algebraic closure of Q in B. *If $\alpha_i \in Q'$ is such that* $\log \alpha_i$ *is defined for $i = 1, \cdots, n$ and if the* $\log \alpha_i$ *are linearly dependent over Q', then they are linearly dependent over Q.* If $B = A$, then $\log = \log_p$. If $B = C$, then log is the usual "multivalued function" for non-zero argument; we assume a fixed determination of $\log \alpha_i$, $i = 1, \cdots, n$.

If $n = 2$, $B = C$, this is Hilbert's 7th problem; if $n = 2$, $B = A$, this is Mahler's theorem. No other cases are known. By the method of Theorem 1′, the conjecture implies $r = r_p$ for all abelian K/Q and all rational primes p. It would also give information even when the galois group G of K/Q is not abelian.

2. Algebraic method

Proof of Theorem 3. We assume $r_p < r$ and derive a contradiction. Let $v_1, \cdots, v_r$ be a basis for a free direct summand of rank r of U. If $u_i = v_i^{p-1}$ then $u_i \in U_p$ for $e = 1, \cdots, r$. Since $r_p < r$, it follows from the definition of r_p that there exist $\alpha_i \in A$ not all zero such that

$$\sum_{i=1}^{r} \alpha_i \log_p \tau(u_i) = 0 \qquad \text{for all } \tau \in T. \tag{6}$$

Let $\theta \in T$ and $L =$ topological closure of $\theta(K)$ in A. L is a galois extension of Q_p with galois group G isomorphic to the galois group of K/Q. In particular we have

$$T = \{g \circ \theta\}_{g \in G}$$

and we may assume each $\alpha_i \in L$ in (6). Thus there exists a minimal non-empty set $R \subseteq \{1, \cdots, r\}$ such that there exist $\alpha_i \in L - 0$ with

$$\sum_{i \in R} \alpha_i \log_p (g \circ \theta(u_i)) = 0 \qquad \text{for } g \in G. \tag{7}$$

Thus

$$0 = h(\sum_{i \in R} \alpha_i \log_p (g \circ \theta(u_i)) = \sum_{i \in R} h(\alpha_i) \log_p (hg \circ \theta(u_i)$$

for all $h, g \in G$ which yields

$$0 = \sum_{i \in R} h(\alpha_i) \log_p (g \circ \theta(u_i)) \qquad \text{for all } h, g \in G. \tag{8}$$

We may combine (7) and (8) to contradict the minimality of R unless $h(\alpha_i) = \alpha_i$ for all $i \in R$ and $h \in G$, i.e. unless $\alpha_i \in Q_p$ for $i \in R$. Thus by changing notation we may there exists $\beta_i \in Z_p$ such that

$$(9) \qquad \log_p \theta(u_1) = \textstyle\sum_{i=2}^r \beta_i \log_p \theta(u_i).$$

We now choose $b_i \in Z$ so that

$$|(\beta_i + b_i)\log_p \theta(u_i)|_p < p^{-2} \qquad \text{for} \quad i = 2, \cdots, n.$$

From (9) we obtain

$$\log_p \theta(u_1 \textstyle\prod_{i=2}^r u_i^{b_i}) = \log_p \theta(u_1) + \textstyle\sum_{i=2}^r b_i \log_p \theta(w_i)$$
$$= \textstyle\sum_{i=2}^r (\beta_i + b_i)\log_p \theta(u_i) = p^2 x$$

where $x \in L$ is such that $|\, x \,|_p < 1$. Let

$$(10) \qquad z = u_1 \textstyle\prod_{i=2}^r u_i^{b_i} \in U_p\,.$$

Thus

$$\log_p \theta(z) = p^2 x = \log_p (\exp(px)^p).$$

Here $y = \exp(px) \in L$ and $|\, y - 1 \,|_p < 1$.

Since $\log_p \theta(z) = \log_p (y^p)$, there exists a root of unity η in L of order a power of p such that $\eta\theta(z) = y^p$. Since the roots of unity of order a power of p in L are already in $\theta(K)$, there exists $i \in Z$ such that $\theta(\zeta^i z) = y^p$.

Let M be the splitting field of $f(x) = x^p - \zeta^i z$ over K. Clearly $M = K$ or $[M:K] = p$. Assume $[M:K] = p$ and let $\alpha \in M$ be a root of $f(x)$. Hence α is a unit and the different of α is $f'(\alpha) = p\alpha^{p-1}$. It follows that the only finite prime of K which can ramify in M is the prime above p; no infinite prime of K can ramify since they must all be complex. But the prime of K above p splits completely in M since $f(x)$ splits completely in L:

$$f(x) = x^p - \zeta^i z = \textstyle\prod_\xi (x - \xi y)$$

where ξ ranges over the *p-th* roots of unity (which are in L). It follows that M is an unramified abelian extension of K. By class field theory [2, Ch. 8, Th. 7], $p = [M:K]$ divides the class number h of K. For $a = 1$, this contradicts the definition of regular prime; for $a > 1$, this contradicts a theorem of Iwasawa [5]. Thus $M = K$, i.e. $\zeta^i z$ is a *p-th* power of an element of K. From (10) $u_i = v_i^{p-1}$, we get

$$\zeta^i z = \zeta^i (v_1 \textstyle\prod_{i=2}^r v_i^{b_i})^{p-1} \in U^p.$$

Let C be the torsion of subgroup of U and denote the residue class of v modulo C by $\mathbf{v}$ (and U/C by $\mathbf{U}$). We have

$$(\mathbf{v}_1 \textstyle\prod_{i=2} \mathbf{v}_i^{b_i})^{p-1} \in \mathbf{U}^p$$

which implies

$$\mathbf{v}_1 \textstyle\prod_{i=2}^r \mathbf{v}_i^{b_i} \in \mathbf{U}^p$$

which contradicts the fact that $\mathbf{v}_1, \cdots, \mathbf{v}_r$ is a Z-basis for $\mathbf{U}$ (since, by definition, $v_1, \cdots, v_r$ is a Z-basis for a free direct summand of rank r of U). This establishes Theorem 3.

Bibliography

1. E. Artin, *Über Einheiten relativ galoisscher Zahlkorper*, J. Reine Angew. Math., vol. 167 (1932), pp. 153–156.
2. E. Artin and J. Tate, *Class field theory*, Harvard Notes, 1961.
3. C. Curtis and I. Reiner, *Representation theory of finite groups and associative algebras*, New York, Interscience, 1962.
4. H. Hasse, *Zahlentheorie*, Berlin, Akademie-Verlag, 1949.
5. K. Iwasawa, *A note on class numbers of algebraic number fields*, Abh. Math. Sem. Univ. Hamburg, vol. 20 (1956), pp. 257–258.
6. H. W. Leopoldt, *Zur Arithmetic in Abelschen Zahlkörpern*, J. Reine Angew. Math., vol. 209 (1962), pp. 54–71.
7. K. Mahler, *Über transzendente P-adische Zahlen*, Compositio Math., vol. 2 (1935), pp. 259–275.
8. ——— , *A correction*, Compositio Math., vol. 8 (1950), pp. 112.
9. H. Minkowski, *Zur Theorie der Einheiten in den algebraische Zahlkörpern*, Göttinger Nachrichten, 1900, p. 90.

Cornell University
Ithaca, New York