145. *On the Class Number of an Absolutely Cyclic Number Field of Prime Degree*

By Norio ADACHI
Department of Mathematics, Tokyo Institute of Technology, Tokyo

(Comm. by Zyoiti SUETUNA, M. J. A., Oct. 13, 1969)

Let K be a cyclic extension of odd prime degree p over $\boldsymbol{Q}$, and suppose that 2 is a primitive root mod p. p may be, for example, 3, 5, 11, 13, 19 or 29. We shall prove that the class number h of K is even, if and only if a cyclotomic unit η of K is either totally positive or totally negative, i.e. $|\eta|$ is totally positive. We shall also show that $|\eta|$ is not totally positive, if the discriminant of K is a power of prime. Hence, in such a case, we can conclude that the class number h of K is odd.

§1. On cyclotomic units.

In order to prove our results, we first recollect some properties of cyclotomic units, which are described in [3] with thorough proofs.

Let K be a cyclic extension of odd prime degree p over $\boldsymbol{Q}$. Then, it is well known that K is cyclotomic, that is, K is contained in $\boldsymbol{Q}_m=\boldsymbol{Q}(\zeta_m)$ for some m. Here, and in what follows, ζ_m denotes

$$\cos\frac{2\pi}{m}+i\sin\frac{2\pi}{m}.$$

Let f be the greatest common divisor of m's such that $\boldsymbol{Q}_m\supset K$. Then, K is contained in $\boldsymbol{Q}_f$. Note that a prime number is ramified in K, if and only if it divides f. For any integer a which is prime to f, we define the element $i(a)$ of the Galois group $G(\boldsymbol{Q}_f/\boldsymbol{Q})$ by

$$\zeta_f^{i(a)}=\zeta_f^a.$$

Then the map

$$a\mapsto i(a)$$

induces an isomorphism of the multiplicative group $\boldsymbol{Z}_f^\times$ of reduced residue classes mod f onto $G(\boldsymbol{Q}_f/\boldsymbol{Q})$. We will use the same notation $i(a)$ for this isomorphism. In general, we will write a for the class of a mod f. Denote by $i_K(a)$ the element of $G(K/\boldsymbol{Q})$ which is induced by $i(a)$. Then, the map

$$a\mapsto i_K(a)$$

induces a homomorphism of $\boldsymbol{Z}_f^\times$ onto $G(K/\boldsymbol{Q})$. We denote by H the kernel of this homomorphism. Since K is real, all elements of K are invariant by $\zeta_f\mapsto\zeta_f^{-1}$. Hence, -1 is contained in H. We take a subset A of H such that $A\cup\{-a\,;\,a\in A\}=H$, and $A\cap\{-a\,;\,a\in A\}=\emptyset$. Let s

be an element of $Z_f^\times$ such that $S=i_K(s)$ generates $G(K/Q)$, and put

$$\eta=\prod_{a\in A}\frac{\zeta_{2f}^{a}-\zeta_{2f}^{-a}}{\zeta_{2f}^{sa}-\zeta_{2f}^{-sa}}=\prod_{a\in A}\frac{\sin\frac{a\pi}{f}}{\sin\frac{sa\pi}{f}}.$$

Then, η is a unit of K, which is called a *cyclotomic unit* of K. We have

$$\eta^{S^\nu}=\prod_{a\in A}\frac{\zeta_{2f}^{s^\nu a}-\zeta_{2f}^{-s^\nu a}}{\zeta_{2f}^{s^{\nu+1}a}-\zeta_{2f}^{-s^{\nu+1}a}}=\prod_{a\in A}\frac{\sin\frac{s^\nu a\pi}{f}}{\sin\frac{s^{\nu+1}a\pi}{f}}. \tag{1}$$

$$(\nu=0,1,\cdots,p-1)$$

For $\alpha\in K^*$, we define

$$\sigma(\alpha)=\begin{cases}0, & \text{if } \alpha>0,\\ 1, & \text{if } \alpha<0.\end{cases}$$

When $\xi_0,\xi_1,\cdots,\xi_{p-1}$ are p units of K, then we define

$$\Sigma(\xi_0,\xi_1,\cdots,\xi_{p-1})=\Sigma(\xi_\nu)\equiv|\sigma(\xi_\nu^{S^\mu})| \qquad (\text{mod } 2).$$

$$(\nu,\mu=0,1,\cdots,p-1)$$

We have $\Sigma(\xi_\nu)\not\equiv 0$ (mod 2), if and only if the signatures of $\xi_0,\xi_1,\cdots,\xi_{p-1}$ are 'independent'.

Let $\varepsilon_1,\cdots,\varepsilon_{p-1}$ be fundamental units of K, and $\varepsilon_0=-1$. Then, we have

$$\Sigma(-1,\eta^S,\cdots,\eta^{S^{p-1}})\equiv h\Sigma \qquad (\text{mod } 2), \tag{2}$$

where $\Sigma=\Sigma(\varepsilon_\nu)$.

§2. Proof.

The theorems to be proved are the following:

Theorem 1. *Let K be a cyclic extension of odd prime degree p over Q, and suppose that* 2 *is a primitive root* mod p, *then the class number h of K is even, if and only if $|\eta|$ is totally positive.*

Theorem 2. *Let K be a cyclic extension of odd prime degree over Q, and suppose that the discriminant of K is a power of prime, then $|\eta|$ is not totally positive.*

Remark. Let K be a cyclic extension of odd prime degree p over Q. Then there exists an integral ideal $\mathfrak{a}$ of Q_p such that $h=N\mathfrak{a}$, where N denotes the absolute norm from Q_p (cf. [2]). Hence, for a prime number l, the l order of h is divisible by the order of l mod p. Thus, 2^{p-1} divides h, if 2 is a primitive root mod p, and if h is even.

Proof of Theorem 1. Put

$$\bar\eta=\begin{cases}-\eta, & \text{if } N\eta=+1,\\ \eta, & \text{if } N\eta=-1.\end{cases}$$

Since the multiplicative group generated by $-1,\bar\eta^S,\cdots,\bar\eta^{S^{p-1}}$ coincides with the multiplicative group generated by $\bar\eta,\bar\eta^S,\cdots,\bar\eta^{S^{p-1}}$, we have

$$\Sigma(-1, \eta^S, \cdots, \eta^{S^{p-1}}) \equiv \Sigma(-1, \bar{\eta}^S, \cdots, \bar{\eta}^{S^{p-1}}) \equiv \Sigma(\bar{\eta}, \bar{\eta}^S, \cdots, \bar{\eta}^{S^{p-1}}) \pmod 2.$$

Hence, from (2), we have

$$\Sigma(\bar{\eta}^{S^\nu}) \equiv h\Sigma \qquad \pmod 2. \tag{3}$$

Put $c_\nu = \sigma(\bar{\eta}^{S^\nu})$, then we have

$$\Sigma(\bar{\eta}^{S^\nu}) \equiv \prod_{i=0}^{p-1} (c_0 + c_1\zeta_p^i + \cdots + c_{p-1}\zeta_p^{i(p-1)}) \qquad \pmod 2.$$

As 2 is a primitive root mod p, 2 inerts in Q_p, i.e., the cyclotomic polynomial $X^{p-1} + X^{p-2} + \cdots + X + 1$ is irreducible (mod 2). Hence, we have

$$c_0 + c_1\zeta_p^i + \cdots + c_{p-1}\zeta_p^{i(p-1)} \equiv 0 \qquad \pmod 2 \qquad \text{for } i \neq 0,$$

if and only if $c_0 = c_1 = \cdots = c_{p-1}$. On the other hand, $\sum_{\nu=0}^{p-1} c_\nu \equiv 1$ (mod 2), since $N\bar{\eta} = -1$. Thus, we see that $|\eta|$ is totally positive, if and only if $\Sigma(\bar{\eta}^{S^\nu}) \equiv 0$ (mod 2).

If $|\eta|$ is not totally positive, then we have $h \equiv 1$ (mod 2) by (3).

Suppose that $|\eta|$ is totally positive, i.e., $\Sigma(\bar{\eta}^{S^\nu}) \equiv 0$ (mod 2). If $\Sigma \equiv 1$ (mod 2), then $h \equiv 0$ by (3). If $\Sigma \equiv 0$ (mod 2), then the signatures of units are not independent. Then, a result of Armitage and Fröhlich ([1]) tells us that h is even.

Proof of Theorem 2. Note that 2 does not ramify in K, if K is cyclic of odd prime degree. Hence, f is odd. We can assume without loss of generality that s and $a(\in A)$ are odd, and that $0 < a < f$. Then, $N\eta = -1$, if (and only if) f is a power of prime (cf. [3], S29). Put

$$g_{s^\nu} = \prod_{a \in A} \sin \frac{s^\nu a\pi}{f}, \quad \nu = 0, 1, 2, \cdots, p.$$

Note that $g = g_{s^0}$ is positive, and $g_{s^p} = -g$, by (1) and by $N\eta = -1$. Hence,

$|\eta|$ is totally positive

$\Longleftrightarrow$ $\eta^{S^\nu} = g_{s^\nu}/g_{s^{\nu+1}}$ is negative for $\nu = 0, 1, \cdots, p-1$,

$\Longleftrightarrow$ $g, g_{s^2}, \cdots, g_{s^{p-1}}$ are positive, and $g_s, g_{s^3}, \cdots, g_{s^p}$ $(=-g)$ are negative.

As $i_K(s)$ generates $G(K/Q)$, $i_K(s^2)$ also generates $G(K/Q)$ and s^2 must be odd. Suppose that $|\eta|$ is totally positive, and put $t = s^2$, then, for another cyclotomic unit $\eta' = g/g_t$, we have $N\eta' = 1$, which gives a contradiction.

References

[1] Armitage-Frölich: Classnumbers and unit signatures. Mathematika, **14**, 94–98 (1967).

[2] Brumer, A.: On the group of units of an absolutely cyclic number field of prime degree. J. Math. Soc. Japan, **21**, 357–358 (1969).
[3] Hasse, H.: Über die Klassenzahl abelscher Zahlkörper, Kapitel II. Berlin (1952).