9. A Note on Class Numbers

By Genjiro FUJISAKI
Department of Mathematics, College of Arts and Sciences,
University of Tokyo

(Communicated by Shokichi IYANAGA, M. J. A., Jan. 12, 1990)

In this paper, we shall make some simple observations on the class numbers of algebraic number fields.

1. For any prime numbers p and q, let

$$d(q,p)=2, \quad \text{for } p=q,$$
$$=\text{the order of } p \bmod q, \quad \text{for } p\neq q$$

and for any integer $n\geq 1$, let

$d(n,p)=$the minimum of $d(q,p)$ for all prime factors q of n.

In his paper ([2], Cor. of Th. 3), Iwasawa proved, as a corollary of his results, the following

Proposition I. Let F be a finite algebraic number field and K a finite Galois extension of F with degree n. Denote by $h(F)$ and $h(K)$ the class numbers of F and K respectively.

Let p be a prime number such that $(p,n)=(p,h(F))=1$. If p divides $h(K)$, then the rank of the Sylow p-subgroup of the ideal class group of K is at least equal to $d(n,p)$.

Applying this proposition and following the argument in a paper of Osada ([3]), we shall prove

Theorem 1. *Let $q\geq 5$ be a prime such that $2q+1$ is also a prime. Let F be a finite algebraic number field with $h(F)=1$ and let K/F be a finite q-extension (i.e., a finite Galois extension with q-power degree).*

Assume $q\nmid h(K)$ and $h(K)<2q+1$, then we have $h(K)=1$.

Proof. Suppose $h(K)>1$, so there exists a prime r $(\neq q)$ such that $r\mid h(K)$. Then, by Prop. I, $r^f\mid h(K)$ where f is the order of $r \bmod q$.

Assumption $h(K)<2q+1$ implies $r^f=1+q$. Since $1+q$ is even, we have $r=2$, so that both $2^f-1=q$ and $2^{f+1}-1=2q+1$ are primes, whence both f and $f+1$ must be prime. This implies $f=2$ and $q=3$, a contradiction.

By a similar (but simpler) argument as above we obtain the following

Proposition 1. *Let q be an odd prime (with no assumption on $2q+1$) and let K/F be a q-extension of number field with $h(F)=1$.*

(i) *Assume $h(K)<q$, then $h(K)=1$.*

(ii) *Assume $(h(K),2)=(h(K),q)=1$ and $h(K)<2q+1$.*
Then, $h(K)=1$.

Let p be a prime and let K/F be a p-extension of number field in which at most one (finite or infinite) prime is ramified. Then, as is well known ([1], [4]), $p\nmid h(F)$ implies $p\nmid h(K)$.

Hence, we obtain the following proposition as a corollary of Theorem 1.

Proposition 2. *Let $q \geq 5$ be a prime such that $2q+1$ is also a prime. Let K/F be a q-extension of number field in which at most one prime is ramified.*

Assume $h(F)=1$ and $h(K)<2q+1$. Then $h(K)=1$.

Let F be a finite number field with $h(F)=1$. Let F_∞/F be a Z_q-extension ($q \geq 3$) and let

$$F=F_0 \subset F_1 \subset \cdots \subset F_n \subset \cdots \subset F_\infty$$

be the sequence of subfields of F_∞/F.

We obtain the following proposition from Props. 1 and 2.

Proposition 3. *Suppose exactly one prime is ramified for F_∞/F. Then*

(i) *$h(F_n)=1$ or $h(F_n)>q$ for every $n \geq 1$.*

(ii) *Suppose, furthermore, $q \geq 5$ and $2q+1$ is also a prime, then $h(F_n) =1$ or $h(F_n) \geq 2q+1$ for every $n \geq 1$.*

2. Let $p>2$ be a prime. For each $n \geq 0$, we denote by K_n^+ the maximal real subfield of the cyclotomic field of the p^{n+1}-th root of unity. K_0^+ is the maximal real subfield of the cyclotomic field of the p-th root of unity.

Since $h(\boldsymbol{Q})=1$ for the rational field $\boldsymbol{Q}$ and only a prime p is ramified for $K_0^+/\boldsymbol{Q}$, we obtain the following result from Prop. 2.

Theorem 2. *Suppose*

(i) *$(p-1)/2$ is a power $q^a (a \geq 1)$ of some prime $q (\geq 5)$,*

(ii) *$2q+1$ is also a prime,*

(iii) *$h(K_0^+)<2q+1$.*

Then $h(K_0^+)=1$.

Corollary (Osada [3]). *Suppose $(p-1)/2$ is a prime q and $h(K_0^+)< p(=2q+1)$. Then, $h(K_0^+)=1$.*

Theorem 3. *Suppose $(p-1)/2$ is a prime. If $h(K_n^+)<p$ for $n \geq 0$, then we have $h(K_n^+)=1$.*

Proof. Sicne $h(K_0^+) \mid h(K_n^+)$, $h(K_0^+)<p$ whence, by the above corollary, $h(K_0^+)=1$. Then, applying Prop. 1, (i) for K_n^+/K_0^+ we have $h(K_n^+)=1$.

The author wishes to thank Professor Iwasawa for his suggestion.

References

[1] K. Iwasawa: A note on class numbers of algebraic humber fields. Abh. Math. Sem. Univ. Hamburg, **20**, 257–258 (1956).

[2] ——: A note on ideal class groups. Nagoya Math. J., **27**, 239–247 (1966).

[3] H. Osada: A remark on the class-number of the maximal real subfield of cyclotomic field. Proc. Japan Acad., **65**A, 318–319 (1989).

[4] L. C. Washington: Introduction to Cyclotomic Fields. Springer-Verlag, New York (1982).