ON THE EXTENSION OF EULER'S CRITERION ABOUT LEGENDRE'S SYMBOL

By SETSUO OHNARI*

Our purpose in this paper is to show two theorems in which Euler's criterion about Legendre's symbol is generalized. In theorem 1 in section 2, using the generalized Legendre's symbol $\left(\frac{a}{k}\right)$ which will be suitably defined in section 2, we shall show

 $\left(\frac{a}{k}\right) \equiv a^{1/2 \cdot \phi(k)} \pmod{k},$

where k is such rational integer as 2^2 or p^r or $2p^r$ (p is an odd prime number, r is an arbitrary positive integer), a is such rational integer as (a, k)=1 and ϕ is Euler's function. In theorem 2 in section 3, using the extended Legendre's symbol $\left(\frac{\alpha}{M}\right)$ which will be suitably defined in section 3, we shall show

 $\left(\frac{\alpha}{M}\right) \equiv \alpha^{1/2 \cdot \phi(M)} \pmod{M},$

where M is integral ideal of quadratic field whose type will be denoted in the table in section 3 and α is such integer of quadratic field as $(\alpha, M)=1$.

In section 1 we shall prove two lemmata about finite Abelian group in preparation for applications in the succeeding sections.

I wish to express my indebtedness to Professor Kazuo Matsuzaka of Hitotsubashi University for many helpful teachings and many useful discussions on the results to be described in this paper.

§1. Lemmata about finite Abelian group.

Let us provide two lemmata about finite Abelian group. We shall use the following notations.

G will denote a finite Abelian group.

e will denote the identity element of G.

S will denote the set of all elements of G whose order is 2.

H will denote a subgroup of *G* such that $\{x \in G; y^2 = x \text{ for some } y \in G\}$

|G|, |S| and |H| will denote the number of elements of G, S and H.

Lemma 1.

$$\prod_{z \in G} z = \begin{cases} a; |S| = 1, S = \{a\}, \\ e; |S| \neq 1. \end{cases}$$

* Assistant Professor (Jokyōju) in Mathematics.

We already showed lemma 1 in [1].

Lemma 2. If |S|=1, $S=\{a\}$, then $x^{|H|} = \begin{cases} a; \ x \in H, \\ e; \ x \in H. \end{cases}$ Proof. Let us define endomorphism f of G such that $f: G \ni x \longrightarrow x^2 \in G$ and then it is plain that

Imf = H, $Ker f = \{e, a\}$.

Therefore it is plain that $|H|=1/2 \cdot |G|$ by $G/\ker f \cong H$.

If $x \in H$, there exists x_0 in G such that $x_0^2 = x$ and it is plain that the all solutions of equation with respect to y, $y^2 = x$ are x_0 and ax_0 . Then let us introduce an equivalence relation in $G - \{x_0, ax_0\}$ as follows,

 $u \sim v \Leftrightarrow u = v \text{ or } uv = x.$

Then it is plain that every equivalence class contains two distinct elements u and vand uv = x. Therefore

 $\prod_{c} z = x^{1/2 \cdot (|G|-2)} \cdot x_0 \cdot a x_0 = a x^{1/2 \cdot |G|} = a x^{|H|}.$ $z \in G$

If $x \notin H$, let us introduce an equivalence relation in G as follows.

 $u \sim v \Leftrightarrow u = v \text{ or } uv = x.$

Then it is plain that every equivalence class contains two distinct elements u and vand uv = x. Therefore

 $\prod z = x^{1/2 \cdot |G|} = x^{|H|}.$ $z \in G$

By the assumption |S|=1, $S=\{a\}$ and lemma 1 Π ~-

$$\prod_{z \in G} z = a$$

Thus we have completed the proof of lemma 2.

§ 2. Generalized Euler's criterion in \mathbb{Z} .

Let us suppose that p is an odd prime number and that a is a rational integer such that (a, p) = 1. Using Legendre's symbol

 $\left(\frac{a}{p}\right) = \begin{cases} +1; & a \text{ is a quadratic residue of } p, \\ -1; & a \text{ is a quadratic non-residue of } p, \end{cases}$

the following Euler's criterion is familiar to us:

$$\left(\frac{a}{p}\right) \equiv a^{1/2 \cdot (p-1)} \pmod{p}.$$

In this section we shall prove Euler's criterion in the case where p is not always prime number. Let \mathbb{Z} be the ring of all rational integers and let k be an element of \mathbb{Z} and let G_k be the group of reduced residue classes of \mathbb{Z} to modulus k. We already showed in [1] that a necessary and sufficient condition that G_k should contain only one involution is

 $k=2^2$ or p^r or $2p^r$,

where p is an odd prime number and r is an positive rational integer and that in this case the involution is the residue class which contain -1.

Let a be an element of \mathbb{Z} such that (a, k) = 1. If the congruence $x^2 \equiv a \pmod{k}$ has

September

at least one solution, we say that a is a quadratic residue of k and if the congruence has no solution, we say that a is a quadratic non-residue of k. So using lemma 2 in the previous section we get

$$a^{1/2 \cdot \psi(k)} = \begin{cases} +1 \pmod{k}; a \text{ is a quadratic residue of } k, \\ -1 \pmod{k}; a \text{ is a quadratic non-residue of } k, \end{cases}$$
(1)

where ϕ is Euler's function.

For a and k which are described above let us define generalized Legendre's symbol such that

 $\left(\frac{a}{k}\right) = \begin{cases} +1; a \text{ is a quadratic residue of } k, \\ -1; a \text{ is a quadratic non-residue of } k. \end{cases}$ (2)

By (1) and (2) we complete a proof of

Theorem 1 (generalized Euler's criterion).

Let $k=2^2$ or p^r or $2p^r$ where p is an odd prime number and r is a positive rational integer. Let a be an element of \mathbb{Z} such that (a, k) = 1. Then

$$\left(\frac{a}{k}\right) = a^{1/2 \cdot \phi(k)} \pmod{k},$$

where ϕ is Euler's function.

§3. Extended Euler's criterion in quadratic field.

In this section we shall consider the above Euler's criterion in quadratic field. We shall use the following notations.

will denote a rational integer which does not contain any square factors m without 1.

$$\omega$$
 will denote \sqrt{m} if $m=2, 3 \pmod{4}$ and $\frac{1+\sqrt{m}}{2}$ if $m=1 \pmod{4}$.

- will denote the ring of all rational integers. \mathbb{Z}
- will denote the field of all rational numbers. O
- will denote the ring of all integers of $\mathbb{Q}(\sqrt{m})$. O_m
- will denote an integral ideal of $\mathbb{Q}(\sqrt{m})$. M
- P, Q and R will denote prime ideals of $\mathbb{Q}(\sqrt{m})$.
- will denote a positive rational integer. r
- $G_m(M)$ will denote the group of reduced residue classes of O_m with respect to modulus M.

Let us call the prime ideal which divides $O_m \cdot 2$ (this means the integral ideal generated by 2 in O_m) even prime ideal and we shall use notations such as P and Q. Let us call the prime ideal which does not divide $O_m \cdot 2$ odd prime ideal and we shall use notation such as R. About even prime ideal we have familiar result:

$$O_m \cdot 2 = \begin{cases} PQ, \ Q = P' \neq P; \ m = 1 \pmod{8} \\ P \qquad ; \ m = 5 \pmod{8} \\ P^2 \qquad ; \ m = 2, \ 3 \pmod{4} \end{cases}$$

where P' will denote a conjugate ideal of P over O_m .

We already showed in [1] that a necessary and sufficient condition that $G_m(M)$ should contain only one involution is that the prime ideal decomposition of M has the type which is shown in the following table, and that in this case the involution is the 1977]

residue class which contains the elements of O_m shown in the following table.

	the type of prime ideal decomposition of M		a representative of the involution of $G_m(M)$
the case in which M does not contain any even prime ideal of O_m	R ^r		-1
the case in which <i>M</i> con- tains several even prime ideals	<i>m</i> ≡1 (mod 8)	PR^{r} QR^{r} PQR^{r} P^{2} Q^{2} $P^{2}Q$ PQ^{2}	-1 -1 -1 -1 -1 -1 -1
	$m \equiv 5 \pmod{8}$	PR ^r	-1
	<i>m</i> ≡2 (mod 4)	P ² P ³ PR ^r	$ \begin{array}{c} 1+\omega \\ -1 \\ -1 \end{array} $
	$m=3 \pmod{4}$	P ² P ³ PR ^r	ω -1 -1

where R is a odd prime ideal, P and Q are even prime ideals, r is a positive rational integer and ω is \sqrt{m} .

Let α be an element of O_m such that $(\alpha, M)=1$. If the congruence $\xi^2 \equiv \alpha \pmod{M}$ has at least one solution, we say that α is a quadratic residue of M and if the congruence has no solution, we say that α is a quadratic non-residue of M. So using lemma 2 in section 1 we get

(i) in the case that α is a quadratic residue of M $\alpha^{1/2 \cdot \phi(M)} \equiv 1 \pmod{M}$,

(ii) in the case that α is a quadratic non-residue of M

$$\alpha^{1/2 \cdot \psi(M)} = \begin{cases} 1 + \omega; \ m \equiv 2 \pmod{4}, \ M = P^2, \\ \omega \ ; \ m \equiv 3 \pmod{4}, \ M = P^2, \\ -1 \ ; \ \text{other cases,} \end{cases}$$

where ϕ is Euler's function.

For α and M which are discribed above let us define extended Legendre's symbol such that

(iii) in the case that α is a quadratic residue of M

$$\left(\frac{\alpha}{M}\right) = 1,$$

(iv) in the case that α is a quadratic non-residue of M $\left(\frac{\alpha}{M}\right) = \begin{cases} 1+\omega; \ m\equiv 2 \pmod{4}, \ M=P^2 \\ \omega \quad ; \ m\equiv 3 \pmod{4}, \ M=P^2 \end{cases}$

$$M = \begin{pmatrix} a & b \\ -1 \end{pmatrix}$$
; other cases.

71

By (i), (ii), (iii) and (iv) we complete a proof of

Theorem 2 (extended Euler's criterion).

Let *M* be a integral ideal of $\mathbb{Q}(\sqrt{m})$ which has the type which is shown in the above table. Let α be an element of O_m such that $(\alpha, M)=1$. Then

 $\left(\frac{\alpha}{M}\right) \equiv \alpha^{1/2 \cdot \phi(M)} \pmod{M},$

where ϕ is Euler's function.

REFERENCES

- [1] Ohnari, S., On the extension of Wilson's theorem to quadratic fields, *Hitotsubashi Journal of Arts and Sciences*, Vol. 18, No. 1, 1977.
- [2] Hardy, G. H. & Wright, E. M., An Introduction to the Theory of Numbers, Oxford, fourth edition, 1960.

(June 14, 1977)

1

72