J. Math. Soc. Japan
Vol. 46, No. 2, 1994

Modular construction of normal basis

By Keiichi KOMATSU

(Received Nov. 17, 1992)

We denote by $\boldsymbol{Q}$ the rational number field and $\boldsymbol{Z}$ the integer ring. Let F be an imaginary quadratic field, p an odd prime number which splits in F, and $\mathfrak{p}$ a prime ideal of F dividing p. For a positive integer m, we denote by $k=F\ (\mathrm{mod}\ \mathfrak{p}^m)$ the ray class field of F modulo $\mathfrak{p}^m$ and by O_k the integer ring of k. Let $K=F\ (\mathrm{mod}\ \mathfrak{p}^{2m})$. In [4], Taylor proved the following striking result:

THEOREM A. *The p-integer ring $O_K[1/p]$ has a normal basis over $O_k[1/p]$.*

The above result represents the first major advance outside cyclotomic case. In this paper, we shall show that we can obtain a better result than Theorem A by a different approach in proving the following theorem:

THEOREM. *Let F be an imaginary quadratic field, p an odd prime number which splits in F, $\mathfrak{p}$ a prime ideal of F dividing p and m a positive integer. Let k and K be the ray class field of F modulo $\mathfrak{p}^m$ and $\mathfrak{p}^{[5m/2]}$, respectively. Then the p-integer ring $O_K[1/p]$ has a normal basis over $O_k[1/p]$.*

This theorem will be proved in two steps, in proving Theorems 1 and 2 stated below. We begin by explaining the notations. We fix a positive integer m, a prime p and put

$$\Gamma=\left\{\begin{pmatrix} a & b \\ c & d \end{pmatrix}\in SL_2(\boldsymbol{Z})\,;\ a\equiv d\equiv 1\ (\mathrm{mod}\ p^m),\ b\equiv 0\ (\mathrm{mod}\ p^m),\ c\equiv 0\ (\mathrm{mod}\ p^{2m})\right\},$$

and

$$S=\left\{\begin{pmatrix} a & b \\ c & d \end{pmatrix}\in\Gamma\,;\ d\not\equiv 1\ \ (\mathrm{mod}\ p^{m+1})\right\}.$$

For an integer n with $n>m$, we put

$$\Gamma_n'=\left\{\begin{pmatrix} a & b \\ c & d \end{pmatrix}\in\Gamma\,;\ a\equiv d\equiv 1\ (\mathrm{mod}\ p^{m+n}),\ b\equiv 0\ (\mathrm{mod}\ p^n),\ c\equiv 0\ (\mathrm{mod}\ p^{m+n})\right\}.$$

Then Γ and Γ_n' are subgroups of $SL_2(\boldsymbol{Z})$ and Γ_n' is a normal subgroup of Γ. Let $\bar{\boldsymbol{Q}}$ be the algebraic closure of $\boldsymbol{Q}$. An element α of $O_{\bar{\boldsymbol{Q}}}[1/p]$ is said to be a p-unit, if α is an invertible element of $O_{\bar{\boldsymbol{Q}}}[1/p]$. For non-negative integer ν, we put $\zeta_\nu=e^{2\pi i/p^\nu}$.