TOKYO J. MATH.
VOL. 19, NO. 1, 1996

On Normal Bases of Some Ring Extensions in Number Fields I

Fuminori KAWAMOTO

Gakushuin University

1. Introduction.

Let k be a number field and K/k a finite Galois extension with Galois group $G=Gal(K/k)$. For a number field N, $\mathfrak{o}_N$ denotes the ring of integers in N. Let S be a finite set of prime ideals of $\mathfrak{o}_k$ that contains all prime ideals which are wildly ramified in K/k. For a finite extension N/k, we simply denote by $\mathfrak{o}_N(S)$ the ring of elements a in N with $\mathrm{ord}_{\mathfrak{P}}(a)\geq 0$ for all prime ideals $\mathfrak{P}$ of $\mathfrak{o}_N$, not lying above S. The field K can be regarded as a module over the group ring kG of G over k by the action $\alpha^\lambda=\sum_{s\in G}a_s\alpha^s$ for $\alpha\in K$ and $\lambda=\sum_{s\in G}a_s s\in kG$. We say that a ring extension $\mathfrak{o}_K(S)/\mathfrak{o}_k(S)$ has a normal basis if $\mathfrak{o}_K(S)$ is a free $\mathfrak{o}_k(S)[G]$-module, that is, there exists some α in $\mathfrak{o}_K(S)$ such that $\{\alpha^s\}_{s\in G}$ is a free $\mathfrak{o}_k(S)$-basis of $\mathfrak{o}_K(S)$. The extension $\mathfrak{o}_K(S)/\mathfrak{o}_k(S)$ is called *ramified* if there exists some prime ideal of $\mathfrak{o}_k$, not belonging to S, which is ramified in K/k (this means that such prime ideal of $\mathfrak{o}_k$ is ramified in the Dedekind ring extension $\mathfrak{o}_K/\mathfrak{o}_k$, as usual). If not so, then it is called *unramified.*

We remark the following fact on the existence of normal bases of extensions of the rings of S-integers which was pointed out by H. Suzuki and whose proof is due to him. It says that we can take a sufficiently large set $U\cup S$, keeping the ramification of primes outside S, such that $\mathfrak{o}_K(U\cup S)/\mathfrak{o}_k(U\cup S)$ has a normal basis.

PROPOSITION 1.1. *Let the notations be as above and $T(\neq\emptyset)$ a finite set of prime ideals of $\mathfrak{o}_k$ that contains all prime ideals, not belonging to S, which are ramified in K/k. Then there exists a finite set U of prime ideals of $\mathfrak{o}_k$ such that $U\cap T=\emptyset$ and $\mathfrak{o}_K(U\cup S)/\mathfrak{o}_k(U\cup S)$ has a normal basis.*

PROOF. Let $V:=\mathfrak{o}_k-\bigcup_{\mathfrak{p}\in T}\mathfrak{p}$ be a multiplicative subset of $\mathfrak{o}_k$ and $V^{-1}\mathfrak{o}_k$ a ring of quotients of $\mathfrak{o}_k$. Then $V^{-1}\mathfrak{o}_k$ is a semi-local ring with maximal ideals $\{\mathfrak{p}\cdot(V^{-1}\mathfrak{o}_k)\}_{\mathfrak{p}\in T}$ and $V^{-1}\mathfrak{o}_K$ is a $(V^{-1}\mathfrak{o}_k)[G]$-module. Since all primes in T are tamely ramified, there exists some α in $\mathfrak{o}_K$ such that $1\otimes\alpha$ is a free generator of $\mathfrak{o}_{k_\mathfrak{p}}\otimes_{\mathfrak{o}_k}\mathfrak{o}_k$ over $\mathfrak{o}_{k_\mathfrak{p}}G$ for each $\mathfrak{p}\in T$ (Cf. [8, Lemma 2.6]), where $\mathfrak{o}_{k_\mathfrak{p}}$ denotes the valuation ring of the completion of

Received October 17, 1994