S. Ullom
Nagoya Math. J.
Vol. 39 (1970), 141-148

INTEGRAL NORMAL BASES IN GALOIS EXTENSIONS OF LOCAL FIELDS

S. ULLOM

Introduction

Throughout this paper F denotes a field complete with respect to a discrete valuation, k_F the residue field of F, K/F a finite Galois extension with Galois group $G = G(K/F)$†. The ring of integers O_K of K contains the (unique) prime ideal $\mathfrak{P}$; the collection of ideals $\mathfrak{P}^n$ for all integers n are ambiguous ideals i.e. G-modules. E. Noether [3] showed K/F tamely ramified implies O_K has an O_F-normal basis, i.e. is isomorphic as an O_FG-module to O_FG itself, O_FG the group ring of G over the ring O_F.

Define subgroups of G

$$G_{i^*} = \{\sigma \in G \mid \forall \alpha \in O_K,\ \sigma\alpha - \alpha \in \mathfrak{P}^{i+1}\},\ i \geqslant 0$$

and

$$G_i^* = \{\sigma \in G \mid \forall \alpha \in K^\times,\ \sigma\alpha/\alpha \in 1 + \mathfrak{P}^i\},\ i \geqslant 1.$$

Then $G_{i^*} \supset G_{i+1}^* \supset G_{i+1^*}$, $i \geqslant 0$, with $G_{i+1}^* = G_{i+1^*}$ written G_{i+1} if the residue field extension k_K/k_F is separable [2, p. 35]. We show (Theorem 3) that an ambiguous ideal $\mathfrak{A}$ of K has an O_F-normal basis iff the trace

$$S_{K/K_1}\mathfrak{A} = \mathfrak{A} \cap K_1,$$

where K_1 is the fixed field of the subgroup G_1^*. This result is obtained from the Galois module structure of $\mathfrak{A} \otimes_{O_F} F$ (resp. $\mathfrak{A} \otimes_{O_F} k_F$) where K/F is tamely ramified (resp. totally and wildly ramified).

Received November 11, 1968.
Revised June 6, 1969.

† Elements of Galois groups act on the left.

This research is supported by National Science Foundation Postdoctoral Fellowship Number 48037.

1. Tamely Ramified Extensions

The following proposition generalizes a result given by Fröhlich [2, p. 22] for rings of integers.

PROPOSITION 1. *An ambiguous ideal $\mathfrak{A}$ of K is $O_F G$-projective iff $\mathfrak{A}$ has an O_F-normal basis.*

Proof. It suffices to consider $\mathfrak{A}$ $O_F G$-projective. For any fractional ideal $\mathfrak{A}$ of K we have $\mathfrak{A}F = K$. Further

$$\mathfrak{A}F \cong \mathfrak{A} \otimes_{O_F} F,$$

where G acts on the righthand side of the above equation by

$$\sigma(\alpha \otimes b) = (\sigma\alpha) \otimes b, \quad \sigma \in G, \quad \alpha \in \mathfrak{A}, \quad b \in F.$$

All isomorphisms are of $O_F G$-modules. By the normal basis theorem for fields

$$K \cong FG \cong O_F G \otimes_{O_F} F.$$

Since O_F is a complete local domain, we may apply Swan's theorem [5, Corollary 6. 4, p. 567] to conclude

$$\mathfrak{A} \cong O_F G.$$

DEFINITION. The extension K/F is *tamely ramified* if the characteristic of k_F does not divide $e(\mathfrak{p}O_K = \mathfrak{P}^e$, $\mathfrak{p}$ the prime ideal of $F)$ and the extension k_K/k_F is separable. We say the extension is *wildly ramified* if it is not tamely ramified.

THEOREM 1. *The extension K/F is tamely ramified iff every ambiguous ideal of K has an O_F-normal basis.*

Proof. If K/F is tamely ramified, then every ambiguous ideal of K is $O_F G$-projective [6, Prop. 1. 3], and hence by Prop. 1 every ambiguous ideal of K has an O_F-normal basis.

Conversely, if every ambiguous ideal of K has an O_F-normal basis, then in particular O_K has a normal basis; it follows that $S_{K/F}O_K = O_F$ and so K/F is tamely ramified.

2. Wildly Ramified Extensions

The field K has a normalized valuation

$$v\colon K^{\times} \to \boldsymbol{Z}$$

with the property $v(\alpha+\beta) \geqslant \operatorname{Inf} v(\alpha),\ v(\beta)$ with equality if $v(\alpha) \neq v(\beta)$, and v extends to K by $v(0) = +\infty$. For an extension K/F define the integers $f(K/F) = [k_K : k_F]$, $e(K/F) = v(\pi_F)$, π_F a prime element of F; finally the different

$$\mathfrak{D}(K/F) = \mathfrak{P}^{m(K/F)}.$$

PROPOSITION 2. *Given the extension K/F with K_1 the fixed field of G_1^*. If $f(K/K_1) > 1$, then $m(K/K_1) \geqslant 2e(K/K_1) - 1$.*

Proof. We use induction on n, $[K : K_1] = p^n$. Of course the characteristic of k_F is p. Set $n = 1$. Then

$$[K : K_1] = f(K/K_1) = p,\quad e(K/K_1) = 1.$$

Since the non-trivial residue field extension is inseparable, $m(K/K_1) \geqslant 1$. Assume for all Galois extensions K/F with $[K : K_1] = p^n$ and $f(K/K_1) > 1$ that $m(K/K_1) \geqslant 2e(K/K_1) - 1$.

Consider K/K_1 Galois of order p^{n+1}, $n \geqslant 1$, $f(K/K_1) > 1$. There exists a subfield K', $K \supset K' \supset K_1$ with $[K : K'] = p^n$ and K'/K_1 Galois. By the tower formula for the different

$$m(K/K_1) = m(K/K') + e(K/K')m(K'/K_1). \tag{1}$$

If the subgroup $H \subset G$ fixes K', then [2, p. 35]

$$H_1^* = H \cap G_1^* = H. \tag{2}$$

Also

$$m(K'/K_1) \geqslant \begin{cases} 2(p-1) & \text{if } e(K'/K_1) = p \\ 1 & \text{if } f(K'/K_1) = p. \end{cases} \tag{3}$$

Suppose $f(K/K') > 1$. Then by (2) we may apply the induction hypothesis to K/K'. So by (1)

$$\begin{aligned} m(K/K_1) &\geqslant 2e(K/K') - 1 + e(K/K')m(K'/K_1) \\ &\geqslant 2e(K/K_1) - 1 \quad \text{by (3).} \end{aligned}$$

If $f(K/K') = 1$, then

$$[K : K'] = e(K/K') = e(K/K_1)$$

and

$$[K' : K_1] = f(K'/K_1) = f(K/K_1).$$

Here $m(K/K') \geqslant 2(e(K/K') - 1)$ and so we have the inequality

$$m(K/K_1) \geqslant 3e(K/K_1) - 2.$$

COROLLARY. *Given extension K/F. If for an ambiguous ideal $\mathfrak{A} = \mathfrak{P}^s$ of K we have $S_{K/K_1}\, \mathfrak{A} = \mathfrak{A} \cap K_1$, then $f(K/K_1) = 1$, $s \equiv 1 \bmod e(K/K_1)$ and $G_2 = \{1\}$.*

Proof. By [6]* we have for $m = m(K/K_1)$, etc.,

$$[(m + s)/e] = 1 + [(s - 1)/e],$$

where $[x]$ denotes the greatest integer less than or equal to x. If $f > 1$, then by Prop. 2

$$[(2e - 1 + s)/e] \leqslant 1 + [(s - 1)/e],$$

which is impossible. Hence $f = 1$, i.e., the residue field extension k_K/k_F is separable. The remainder of the Corollary follows from [6, Theorem 2. 1].

q. e. d.

Cardinality of a finite set S is Card S and R^t is the product of t copies of a ring R. For a G-module M, M^G denotes the group of fixed points under the action of G. When $f(K/K_1) = 1$, $G^*_{i+1} = G_{i+1^*}$, $i \geqslant 0$, and we write G_{i+1}.

PROPOSITION 3. *Given the extension K/K_1 with $f(K/K_1) = 1$ and $G_2 = \{1\}$. Then the dimension of $(\mathfrak{P}/\mathfrak{p}\mathfrak{P})^{G_1}$ $(\mathfrak{p} = \mathfrak{P} \cap K_1)$ as a vector space over $k = k_{K_1}$ is one.*

Proof. The result is obviously true for $G_1 = \{1\}$, so take $G_1 \neq \{1\}$. Use the notation that for $\alpha, \beta \in O_K$, $\alpha \equiv \beta$ means $\alpha \equiv \beta \bmod \mathfrak{P}^{1+e}$, where $e = \operatorname{Card} G_1$; also characteristic of k is p. Choose a prime element π of K. Since $G_2 = \{1\}$, for $\sigma \neq 1$

$$\sigma\pi = \pi(1 + \alpha(\sigma)), \quad \sigma \in G_1, \quad \alpha(\sigma) \in O_K, \quad v(\alpha(\sigma)) = 1. \tag{4}$$

For $1 \leq i \leq e - 1$, $i = p^c n$, $p \nmid n$, we have by (4) and the binomial expansion for $\sigma \neq 1$

* In [6] there is an *a priori* assumption of separability of residue field extensions; the results needed in this paper from [6] are seen immediately not to require this assumption.

$$\sigma\pi^i - \pi^i \equiv \pi^i\,(n\alpha(\sigma)^{p^c} + \cdots + \alpha(\sigma)^i) \tag{5}$$
$$= \pi^{i+p^c}(n\beta(\sigma)^{p^c}) + \text{higher order terms}$$

where $\alpha(\sigma) = \beta(\sigma)\pi$. Thus for $1 \leq i \leq e-1$

$$v(\sigma\pi^i - \pi^i) = i + p^c$$

and for $1 \leqslant i \leqslant e$

$$\sigma\pi^i - \pi^i \equiv 0 \text{ iff } i = e.$$

Thus the dimension of $(\mathfrak{P}/\mathfrak{p}\mathfrak{P})^{G_1}$ is at least one. It remains to show given $\gamma \in O_K$ with $1 \leqslant v(\gamma) < e$, that there exists $\sigma \in G_1$ such that $\sigma\gamma \not\equiv \gamma$. Since $[K : K_1] = e(K/K_1)$, the elements $\pi, \cdots, \pi^e$ are an O_{K_1}-basis of $\mathfrak{P}$ and hence their images in $\mathfrak{P}/\mathfrak{p}\mathfrak{P}$ are a k-basis. We may write $\gamma \equiv \sum_{i=1}^{e} a_i\pi^i$, $a_i = 0$ or unit of O_{K_1}. For some $\sigma \neq 1$ set

$$u = \operatorname*{Inf}_{1 \leqslant i \leqslant e-1} v(a_i(\sigma\pi^i - \pi^i)).$$

Set

$$\delta(\sigma) = \sum_{j=1}^{b} a_{\nu_j}(\sigma\pi^{\nu_j} - \pi^{\nu_j}),\ \nu_1 < \cdots < \nu_b \text{ if } b > 1,$$

where the summation is over all $1 \leqslant i \leqslant e-1$ with $v(a_i(\sigma\pi^i - \pi^i)) = u$; set $\nu_j = p^{c_j}n_j$, $p \nmid n_j$. Note $c_1 > \cdots > c_b$ if $b > 1$. From (5)

$$\delta(\sigma) = \pi^u h(\beta(\sigma)) + \text{higher order terms } (\delta(1) = \beta(1) = 0)$$

where the polynomial

$$h(X) = \sum_{j=1}^{b} a_{\nu_j} n_j X^{p^{c_j}}.$$

Denote by $\bar{h}(X)$ the image of the polynomial $h(X)$ in the polynomial ring $k[X]$.

Assume $\forall\sigma \in G_1$, $\sigma\gamma \equiv \gamma$; then $\forall\sigma \in G_1$, $v(\delta(\sigma)) \geqslant u+1$ since $u \leqslant e$. Hence $\forall\sigma \in G_1$, $v(h(\beta(\sigma))) \geqslant 1$. In general we have the homomorphism of G_1 into the additive group of $O_K/\mathfrak{P}$ given by $\sigma \to \bar{\beta}(\sigma)$ when $\sigma \in G_1$ and $\bar{\beta}(\sigma)$ is the image of $\beta(\sigma) \in O_K$ in $O_K/\mathfrak{P}$. The kernel is G_2 which is trivial by hypothesis. For another prime element π of K, the $\bar{\beta}(\sigma)$ are determined up to multiplication by a unit of $O_K/\mathfrak{P}$, but we are interested only in the number of distinct $\bar{\beta}(\sigma)$, $\sigma \in G_1$. The condition $\forall\sigma \in G_1$, $v(h(\beta(\sigma))) \geqslant 1$, becomes in the field $O_K/\mathfrak{P}$

$$\bar{h}(\bar{\beta}(\sigma)) = 0 \quad \forall\sigma \in G_1. \tag{6}$$

For any choice of prime element π of K the polynomial $\bar{h}(X)$ has degree less than or equal to e/p but has e(distinct) roots by (6). This is impossible since $\bar{h}(X)$ is not the zero element of $k[X]$; so there exists $\sigma \in G_1$ such that $\sigma\gamma \not\equiv \gamma$.

For completeness we include a proof of the following well-known proposition; see e.g. [1, § 3, Exercise 13] for a partial statement.

PROPOSITION 4. *Let R be a discrete valuation ring with residue field $k = R/\mathfrak{p}$ of characteristic $p > 0$. Let G be a finite p-group and M an RG-module which is R-projective and of R-rank Card G. The following are equivalent:*

(i) *$\dim (M/\mathfrak{p}M)^G = 1$ ($\dim$ = vector space dimension over k).*

(ii) *$M \cong RG$ as RG-modules.*

Proof. (ii) implies (i) is clear, so we consider only (i) implies (ii). Let W be a kG-module with dim W finite, I the two-sided nilpotent ideal which is the kernel of the augmentation homomorphism

$$\varepsilon : kG \rightarrow k, \quad \varepsilon(\sum a_\sigma \sigma) = \sum a_\sigma, \quad a_\sigma \in k.$$

From now on we will assume $\dim W/IW$ to be one. Define the map ϕ as the composite

$$kG \xrightarrow{\varepsilon} k \xrightarrow{\approx} W/IW.$$

We have the diagram of kG-modules with exact row

$$\begin{tikzcd} & & & kG \arrow[d, "\phi"] & \\ O \arrow[r] & IW \arrow[r] & W \arrow[r, "\psi"] & W/IW \arrow[r] & O. \end{tikzcd}$$

There exists a kG-linear map $\theta : kG \rightarrow W$ with $\psi\theta = \phi$ since kG is projective over itself. Use I nilpotent to show θ surjective. Further if $\dim kG = \dim W$, θ is also injective and therefore an isomorphism.

Thus if we set $M/\mathfrak{p}\ M = W$, we have $M/\mathfrak{p}\ M \cong kG$. Use M is R-projective and the standard argument with Nakayama's lemma to show $M \cong RG$.

q. e. d.

Putting together Propositions 3 and 4 and noting $\mathfrak{P}$ is O_{K_1}-projective, we have proved the following theorem.

THEOREM 2. *Given the extension K/K_1 with $f(K/K_1) = 1$ and $G_2 = \{1\}$. Then the ambiguous ideal $\mathfrak{P}$ of K has an O_{K_1}-normal basis.*

3. Arbitrary Extensions

Given a commutative ring R with 1 and finite group G. An RG-module M is relatively RG-projective* if there exists an R-endomorphism ϕ of M with $S_G(\phi) = 1_M$, i.e.

$$\sum_{\sigma \in G} \sigma(\phi(\sigma^{-1}m)) = m \quad \forall m \in M.$$

PROPOSITION 5. *Given an extension K/F, H a subgroup of the Galois group G with fixed field L. Suppose L/F is tamely ramified. If an ambiguous ideal $\mathfrak{A}$ of K is relatively $O_L H$-projective, then it is $O_F G$-projective.*

Proof. By hypothesis there exists an O_L-endomorphism ψ of $\mathfrak{A}$ with $S_H(\psi) = 1_{\mathfrak{A}}$. L/F tamely ramified implies there exists $\beta \in O_L$ with $S_{L/F}(\beta) = 1$. Denote also by β the endomorphism of $\mathfrak{A}$ given by multiplication by β. Then for the O_F-endomorphism $\psi . \beta$ of $\mathfrak{A}$ a short computation shows $S_G(\psi . \beta) = 1_{\mathfrak{a}}$. So $\mathfrak{A}$ is relatively $O_F G$-projective. On the other hand, $\mathfrak{A}$ is O_F-projective and thus $O_F G$-projective [4, Prop. 2. 3, p. 702].

We can now prove the main result.

THEOREM 3. *An ambiguous ideal $\mathfrak{A}$ of the extension K over F has an O_F-normal basis iff $S_{K/K_1}\mathfrak{A} = \mathfrak{A} \cap K_1$.*

Proof. If $\mathfrak{A}$ has a normal basis, then it is easy to see that $S_{K/K_1}\mathfrak{A} = \mathfrak{A} \cap K_1$. Conversely, assume $S_{K/K_1}\mathfrak{A} = \mathfrak{A} \cap K_1$. Take $G_1^* \neq \{1\}$, otherwise we are done by Theorem 1. By the Corollary to Prop. 2, $f(K/K_1) = 1$, $\mathfrak{A} = \mathfrak{P}^s \cong \mathfrak{P}$ as $O_{K_1}G_1$-modules. By Theorem 2 $\mathfrak{P} \cong O_{K_1}G_1$. Since K_1/F is tamely ramified, we apply Prop. 5 to conclude $\mathfrak{A}$ is $O_F G$-projective. Then Prop. 1 shows $\mathfrak{A} \cong O_F G$.

REFERENCES

[1] N. Bourbaki, *Algèbre Commutative,* Actualités scientifiques et industrielles 1290, Hermann, Paris, 1961, Chapitre 2.

[2] A. Fröhlich, *Local Fields, Algebraic Number Theory,* Academic Press, London, 1967.

* See [4] for the needed results on relatively (weakly) projective modules over group rings.

[3] E. Noether, Normalbasis bei Körpern ohne höhere Verzweigung, J. reine angew. Math. **167** (1931), 147–152.

[4] D.S. Rim, Modules over finite groups, Ann. of Math. **69** (1959), 700–712.

[5] R. Swan, Induced representations and projective modules, Ann. of Math. **71** (1960), 552–578.

[6] S. Ullom, Normal bases in Galois extensions of number fields, Nagoya Math. J. **34** (1969), 153–167.

University of Illinois
Urbana, Illinois