S. Ullom
Nagoya Math. J.
Vol. 34 (1969), 153–167

NORMAL BASES IN GALOIS EXTENSIONS OF NUMBER FIELDS

S. ULLOM*

Introduction

The notion of module together with many other concepts in abstract algebra we owe to Dedekind [2]. He recognized that the ring of integers O_K of a number field was a free $\boldsymbol{Z}$-module. When the extension K/F is Galois, it is known that K has an algebraic normal basis over F. A fractional ideal of K is a Galois module if and only if it is an ambiguous ideal. Hilbert [4, §§105–112] used the existence of a normal basis for certain rings of integers to develop the theory of root numbers—their decomposition already having been studied by Kummer.

Let K/F be a Galois extension of number fields. A necessary condition that O_K have a normal basis was given by Speiser [9], namely that K/F be tamely ramified. Hilbert [4, Theorem 132] showed O_K has a normal basis when $K/\boldsymbol{Q}$ is abelian and the degree of $K/\boldsymbol{Q}$ is prime to the discriminant of $K/\boldsymbol{Q}$. E. Noether [7] proved that if K/F is tamely ramified, then O_K has a normal basis everywhere locally. When $K/\boldsymbol{Q}$ is abelian with $G = G(K/\boldsymbol{Q})$, Leopoldt [6] gave a complete structure theory for O_K as a $\boldsymbol{Z}G$-module using Gauss sums as generators. His theory uses in a crucial way Kronecker's theorem that every absolutely abelian field is a subfield of a cyclotomic field and that the base ring of integers $\boldsymbol{Z}$ is a principal ideal ring. Fröhlich [3] using "Kummer invariants" considered the case when K/F is a Kummer extension and gave necessary and sufficient conditions that O_K have a normal basis. Yokoi [11] using the structure theory of integral representations of cyclic groups of prime order described the integral representations afforded by O_K, $K/\boldsymbol{Q}$ a cyclic extension of prime degree.

Received October 16, 1967.
Revised July 15, 1968.
* This research is partially supported by National Science Foundation Contract Number GP-1837 and GP-6010.

https://doi.org/10.1017/S0027763000024521 Published online by Cambridge University Press

Here we continue the study of the relationship between module structure and arithmetic properties. We consider all ambiguous ideals of K, not just the ring of integers of K, as Galois modules. In Chapter I the question of existence of normal bases of ambiguous ideals in tamely ramified abelian extensions of the rationals is reduced to the corresponding question for ambiguous ideals of the cyclotomic field $\boldsymbol{Q}(l)$ of l-th roots of unity over $\boldsymbol{Q}$. A sufficient condition for all the ambiguous ideals in a cyclic extension of the rationals of prime degree to have a normal basis is given in Theorem 1. 10. (All field extensions are assumed finite and all modules finitely generated over their ring.)

Chapter II gives necessary conditions for an ambiguous ideal in a wildly ramified Galois extension to have a normal basis; among them is the triviality of a second ramification group. These conditions are sufficient for abelian extensions of $\boldsymbol{Q}$ and quadratic extensions of $\boldsymbol{Q}(\sqrt{-1})$. The latter statement is proven in the author's thesis.

Chapter I. Normal bases in abelian extensions of the rationals

We begin the chapter with some general properties of ambiguous ideals. Let K/F be a Galois extension with Galois group G, F the quotient field of a Dedekind domain O_F, O_K the integral closure of O_F in K. Residue class field extensions are assumed separable. The ring of integers O_K is a Dedekind domain and a G-module under Galois action. For $\beta \in K$ and $\sigma \in G$ we denote either by $\sigma\beta$ or β^σ the action of σ on β. If $\tau \in G$, we write $(\beta^\tau)^\sigma = \beta^{\tau\sigma}$.

DEFINITION. Let $\mathfrak{P}$ be a prime ideal of K with ramification index e over F. $\mathfrak{P}$ is *tamely ramified* over F if the characteristic of the field $\mathrm{O}_F/\mathfrak{P} \cap \mathrm{O}_F$ is prime to e. If every prime of K is tamely ramified over F, K/F is said to be tamely ramified. Prime ideal of F (resp. K) means prime ideal of O_F (resp. O_K). An ideal $\mathfrak{A}$ (possibly fractional) of K is *G-ambiguous* or simply *ambiguous* if $\mathfrak{A}$ is a G-module.

Let $\mathfrak{p}$ be a prime ideal of F decomposing in K as $\mathfrak{p}\mathrm{O}_K = (\mathfrak{P}_1 \cdots \mathfrak{P}_g)^e$. Set $\psi(\mathfrak{p}) = \mathfrak{P}_1 \cdots \mathfrak{P}_g$. It is known that

(i) $\psi(\mathfrak{p})$ is ambiguous and the set of all $\psi(\mathfrak{p})$, $\mathfrak{p}$ prime in F, is a free basis for the group of ambiguous ideals of K,

https://doi.org/10.1017/S0027763000024521 Published online by Cambridge University Press

(ii) An ambiguous ideal $\mathfrak{A}$ of K may be put in the form $\mathfrak{A}_0\mathfrak{b}$ where $\mathfrak{b}$ = ideal of F,

$$\mathfrak{A}_0 = \psi(\mathfrak{p}_1)^{a_1} \cdots \psi(\mathfrak{p}_t)^{a_t}, \quad 0 \leq a_i < e_i,$$

where $e_i > 1$ is the ramification index of a prime of K dividing $\mathfrak{p}_i$. $\mathfrak{A}$ determines $\mathfrak{A}_0$ and $\mathfrak{b}$ uniquely. $\mathfrak{A}_0$ is called a *primitive ambiguous ideal.* For $\mathfrak{A}$ ambiguous, $\psi(\mathfrak{p})^u \| \mathfrak{A}$ shall mean $\mathfrak{P}^u \| \mathfrak{A}$, $\mathfrak{P}$ any prime of K dividing $\mathfrak{p}$, where u may be negative.

We now determine the trace $S_{K/F}\mathfrak{A}$ of an ambiguous ideal $\mathfrak{A}$ of K. Since the trace function $S = S_{K/F}$ is F-linear, $S\mathfrak{A}$ is an ideal of F. Let $\mathfrak{p}$ be an arbitrary prime ideal of F with $\mathfrak{p}O_K = \psi(\mathfrak{p})^e$, $\psi(\mathfrak{p})^s \| \mathfrak{A}$, and $\psi(\mathfrak{p})^m \| \mathfrak{D}(K/F)$ the relative different of K/F. $[x]$ denotes the greatest integer less than or equal to the real number x. The next proposition generalizes a result of Yokoi [12, Prop. 2, p. 209].

1. 1. PROPOSITION. *Take K/F as in the first paragraph of this chapter; let $\mathfrak{A}$ be an ambiguous ideal of K and $\mathfrak{p}$ a fixed but arbitrary prime ideal of F. The $\mathfrak{p}$-component of $S\mathfrak{A}$ is $\mathfrak{q}^r$ where $\mathfrak{p}^r$ is the highest power of $\mathfrak{p}$ dividing $\mathfrak{A}\mathfrak{D}(K/F)$.*

Proof. For any ideal $\mathfrak{b}$ of F, $\mathfrak{b}_\mathfrak{p}$ denotes the $\mathfrak{p}$-component of $\mathfrak{b}$.

For ideals $\mathfrak{A}$ of K, $\mathfrak{b}$ of F we have $S\mathfrak{A} \subseteq \mathfrak{b} \iff \mathfrak{A} \subseteq \mathfrak{b}\mathfrak{D}^{-1}(K/F)$. If r is an integer, this means

$$(S\mathfrak{A})_\mathfrak{p} \subseteq \mathfrak{p}^r \iff s \geq er - m \iff r \leq (m+s)/e.$$

The maximum integer r satisfying this is $r = [(m+s)/e]$.

1. 2. COROLLARY. *If K/F is tamely ramified, then $S\mathfrak{A} = \mathfrak{A} \cap F$.*

Proof. The $\mathfrak{p}$-component of $\mathfrak{A} \cap F$ is $\mathfrak{p}^y$ where

$$y = [(e - 1 + s)/e].$$

Since K/F is tamely ramified, $m = e - 1$. By 1. 1 the $\mathfrak{p}$-component of $S\mathfrak{A}$ is $\mathfrak{p}^r$ where

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

Now use the fact that in a Dedekind domain an ideal may be written uniquely as a product of powers of prime ideals.

We now make some observations on ambiguous ideals as Galois modules.

https://doi.org/10.1017/S0027763000024521 Published online by Cambridge University Press

1. 3. PROPOSITION. *Suppose $G = G(K/F)$ and H is a subgroup of G. K/F tamely ramified implies any ambiguous ideal $\mathfrak{A}$ of K is $O_F H$-projective.*

Proof. By Rim [8, Prop. 2. 3, p. 702] it is enough to show $\mathfrak{A}$ is O_F-projective and there exists an O_F-endomorphism $\rho: \mathfrak{A} \to \mathfrak{A}$ such that $\sum_{\sigma \in H} \sigma\rho(\sigma^{-1}\alpha) = \alpha$ for all $\alpha \in \mathfrak{A}$.

Since $\mathfrak{A}$ is a finitely generated torsion-free O_F-module, $\mathfrak{A}$ is O_F-projective. Let L be the fixed field of H. K/F tamely ramified implies K/L tamely ramified. Thus $\exists \beta \in O_K$ with $S_{K/L}(\beta) = 1$. Now take ρ to be multiplication by β.

1. 4. COROLLARY. *$\mathfrak{A}$ is cohomologically trivial as a G-module.*

DEFINITION. An ideal $\mathfrak{A}$ of K has an *$O_F G$-normal basis* if $\mathfrak{A}$ is isomorphic to the group ring $O_F G$ (isomorphism of $O_F G$-modules); equivalently $\exists \alpha \in \mathfrak{A}$ such that every element of $\mathfrak{A}$ may be put in the form $\sum_{\sigma \in G} a_\sigma \alpha^\sigma, a_\sigma \in O_F$. The notation for this will be $\mathfrak{A} = O_F G \cdot [\alpha]$. We may also say $\mathfrak{A}$ has a K/F-normal basis, or simply normal basis and write $\mathfrak{A} = [\alpha]$. Note $\mathfrak{A}$ is ambiguous if it has a normal basis.

In 1. 5 and 1. 6 L is an intermediate field $F \subseteq L \subseteq K$, fixed by the normal subgroup $H \subseteq G$.

1. 5. *Remark.* (i) If an ideal $\mathfrak{A}$ of K is G-ambiguous, then $\mathfrak{A} \cap L$ is G/H-ambiguous.

(ii) If an ideal $\mathfrak{b}$ of L is G/H-ambiguous, then the extended ideal $\mathfrak{b}O_K$ of K is G-ambiguous.

1. 6. PROPOSITION. *If $\mathfrak{A} = O_F G \cdot [\alpha]$, then $\mathfrak{A} \cap L = O_F(G/H) \cdot [S_{K/L}(\alpha)]$.*

Proof. $\mathfrak{A} \cap L$ is a G/H-module, since H acts trivially on $\mathfrak{A} \cap L$. Write $\beta \in \mathfrak{A}$ as $\sum_{\tau \in G} a_\tau \alpha^\tau$, $a_\tau \in O_F$.

$$\beta^\sigma = \sum_\tau a_\tau \alpha^{\tau\sigma} = \sum_\tau a_{\tau\sigma^{-1}} \alpha^\tau.$$

If $\beta \in \mathfrak{A} \cap L$, then $\beta^\sigma = \beta$ for $\sigma \in H$; consequently, $\sigma \in H$ implies $a_\tau = a_{\tau\sigma^{-1}}$, i.e., $a_\tau = a_{\tau\sigma}$. For $\beta \in \mathfrak{A} \cap L$,

$$\beta = \sum_{\tau/H} a_\tau \sum_{\sigma \in H} \alpha^{\tau\sigma} = \sum_{\tau/H} a_\tau S_{K/L}(\alpha^\tau),$$

https://doi.org/10.1017/S0027763000024521 Published online by Cambridge University Press

where $\sum_{\tau/H}$ denotes a sum over a complete set of coset representatives for G/H.

Note $S_{K/L}(\alpha) \in \mathfrak{A} \cap L$. Since $S_{K/L}(\alpha^\tau) = (S_{K/L}(\alpha))^\tau$, we conclude

$$\mathfrak{A} \cap L = O_F(G/H) \cdot [S_{K/L}(\alpha)].$$

1. 7. *Remark.* Take K/F as in the first paragraph of this chapter, $\mathfrak{A}$ an ambiguous ideal of K. Suppose $\mathfrak{A} = O_F G \cdot [\alpha]$ for some $\alpha \in \mathfrak{A}$. If $\mathfrak{b}$ is a principal ideal (b) of F, then the ideal $\mathfrak{b}\mathfrak{A} = O_F G \cdot [b\alpha]$.
As a consequence, we see that if O_F is a principal ideal domain, the problem of showing an ambiguous ideal has a normal basis reduces to the corresponding problem for primitive ambiguous ideals.

1. 8. PROPOSITION. *Let F be an algebraic number field with K_1, K_2 Galois extensions of F such that $K_1 \cap K_2 = F$ and the discriminants $D_i = D(K_i/F)$, $i = 1, 2$, are relatively prime. Let $\mathfrak{A}_i$ be an integral ambiguous ideal of K_i with $\mathfrak{A}_i = O_F G_i \cdot [\alpha_i]$, $\alpha_i \in \mathfrak{A}_i$, where $G_i = G(K_i/F)$. Then the ambiguous ideal $\mathfrak{A}_1\mathfrak{A}_2$ of $L = K_1K_2$ has a normal basis*, i.e., $\mathfrak{A}_1\mathfrak{A}_2 = O_F G \cdot [\alpha_1\alpha_2]$, *where $G = G_1 \times G_2 = G(L/F)$, $\sigma = (\sigma_1, \sigma_2) \in G_1 \times G_2$ acts on $\alpha_1\alpha_2$ by*

$$\sigma(\alpha_1\alpha_2) = (\sigma_1\alpha_1)(\sigma_2\alpha_2).$$

Proof. Let $\sigma_j^{(i)}$, $j = 1, \cdots, m_i$, be the distinct F-autmorphisms of K_i, $i = 1, 2$. The square of the determinant

$$\Delta[\alpha_i] = \det(\sigma_j^{(i)}\sigma_k^{(i)}\alpha_i), \quad i = 1, 2,$$

is the discriminant (with respect to K_i/F) of the $O_F G_i$-module generated by α_i. Let $\mathfrak{C} = \mathfrak{A}_1\mathfrak{A}_2$ (in O_L). We have

$$D_{L/F}(\mathfrak{C}) = (N_{L/F}\mathfrak{C})^2 D(L/F)$$

and

$$N_{L/F}\mathfrak{C} = (N_{K_1/F}\mathfrak{A}_1)^{m_2}(N_{K_2/F}\mathfrak{A}_2)^{m_1}.$$

Set $M = O_F G \cdot [\alpha_1\alpha_2]$. Clearly $M \subseteq \mathfrak{C}$. It suffices to show the discriminants of M and $\mathfrak{C}$ coincide as ideals of O_F. The relative discriminant of M is $\Delta[\alpha_1\alpha_2]^2$. One finds

https://doi.org/10.1017/S0027763000024521 Published online by Cambridge University Press

$$\begin{aligned}\Delta[\alpha_1\alpha_2]^2 &= \Delta[\alpha_1]^{2m_2}\Delta[\alpha_2]^{2m_1}\\ &= (N_{K_1/F}\mathfrak{A}_1)^{2m_2}(N_{K_2/F}\mathfrak{A}_2)^{2m_1}D_1^{m_2}D_2^{m_1}\\ &= D(L/F)(N_{L/F}\mathfrak{C})^2.\end{aligned}$$

One uses D_1, D_2 relatively prime to obtain the last equality.

The assertions on the Galois group $G(L/F)$ follow at once from the shifting theorem of Galois theory.

We now restrict our attention to cyclotomic extensions. Let F be an extension of the rationals $\boldsymbol{Q}$. Assume K/F is an abelian extension. From class field theory there exists in F the congruence ideal group $H_{\mathfrak{f}}$ with conductor $\mathfrak{f}$ to which K is the class field. For $\mathfrak{p}$ a finite prime of F ramified in K, $\mathfrak{p}$ is tamely ramified in K/F if and only if $\mathfrak{p}\|\mathfrak{f}$.

Consider $K/\boldsymbol{Q}$ abelian. K is class field to the congruence ideal group H_m; m(resp. mp_∞) is the conductor for K real (resp. imaginary), and $K\subseteq\boldsymbol{Q}(m)$, the cyclotomic field of m-th roots of unity over the rationals. If $K/\boldsymbol{Q}$ is tamely ramified, then $m = l_1\cdots l_r$, a product of distinct odd primes. Thus

$$K\subseteq\boldsymbol{Q}(l_1\cdots l_r) = \boldsymbol{Q}(l_1)\cdots\boldsymbol{Q}(l_r).$$

Let p be a rational prime and consider its decomposition in $\boldsymbol{Q}(m)$:

$$p\mathrm{O}_{\boldsymbol{Q}(m)} = (\mathfrak{P}_1\cdots\mathfrak{P}_g)^{e(p)} = \psi(p)^{e(p)}.$$

For a primitive ambiguous ideal $\mathfrak{A}$ of $\boldsymbol{Q}(m)$ we have

$$\mathfrak{A} = \psi(l_1)^{a_1}\cdots\psi(l_r)^{a_r},\quad 0\leq a_i < e(l_i).$$

Denote by $\mathfrak{l}_i$ the unique prime ideal of $\boldsymbol{Q}(l_i)$ dividing l_i. With these notations $\mathfrak{l}_1^{a_1}\mathfrak{l}_2^{a_2}$ as an ideal of $\boldsymbol{Q}(l_1)\boldsymbol{Q}(l_2) = \boldsymbol{Q}(l_1l_2)$ is $\psi(l_1)^{a_1}\psi(l_2)^{a_2}$, since no ramification over $\mathfrak{l}_i$ occurs in $\boldsymbol{Q}(l_il_j)/\boldsymbol{Q}(l_i)$, $i\neq j$. Repeat this argument for the successive composites of $\boldsymbol{Q}(l_1\cdots l_i)$ and $\boldsymbol{Q}(l_{i+1})$, $i = 1,\cdots, r-1$. Finally note that $\boldsymbol{Q}(m)$ is the composite of r linearly disjoint fields $\boldsymbol{Q}(l_i)$, whose absolute discriminants are relatively prime in pairs. Thus 1. 8 applies, and we have proven the following formal reduction theorem.

1. 9. THEOREM. *Suppose $K/\boldsymbol{Q}$ is abelian and tamely ramified, so $K\subseteq L = \boldsymbol{Q}(l_1\cdots l_r)$, l_i distinct odd primes. Let $\mathfrak{l}_i$, $i = 1,\cdots, r$, be the prime ideal of $\boldsymbol{Q}(l_i)$ dividing l_i and let $\mathfrak{A}$ be an ambiguous ideal of L which is the product of powers of $\mathfrak{l}_i$ (extended to O_L), i.e., $\mathfrak{A} = \prod_i \mathfrak{l}_i^{j}$, $j = j(i)$. If each factor $\mathfrak{l}_i^{j}$ of $\mathfrak{A}$*

https://doi.org/10.1017/S0027763000024521 Published online by Cambridge University Press

has a normal basis in $\boldsymbol{Q}(l_i)$, *then* $\mathfrak{A} \subseteq L$ *has a normal basis. Consequently, the ambiguous ideal* $\mathfrak{A} \cap K$ *of* K *has a normal basis.*

In order to give a criterion for the existence of normal bases in cyclic extensions of prime degree we define the projective class group $P(R)$ of a ring R with 1 [8]. Two projective R-modules P_1, P_2 are equivalent if and only if there exist free R-modules F_1, F_2 with $P_1 \oplus F_1 \cong P_2 \oplus F_2$. (All modules are assumed finitely generated over R.) This set of classes of R-modules becomes an abelian group when the law of composition is given by direct sum of R-modules.

Rim [8, Theorem 6. 24, p. 711] has shown for R the group ring $\boldsymbol{Z}G$ where G is a cyclic group of prime order l and $\boldsymbol{Z}$ the rational integers that $P(\boldsymbol{Z}G)$ is isomorphic to the ideal class group of the field $\boldsymbol{Q}(l)$. Further the identity element of $P(\boldsymbol{Z}G)$ consists only of free $\boldsymbol{Z}G$-modules.

Let $F/\boldsymbol{Q}$ be a tamely ramified cyclic extension of prime degree l. Any ambiguous ideal $\mathfrak{A}$ of F is $\boldsymbol{Z}G$-projective by 1. 3 where $G = G(F/\boldsymbol{Q})$. If $\boldsymbol{Q}(l)$ has class number one, it follows from Rim's result that $\mathfrak{A}$ is $\boldsymbol{Z}G$-free and hence has a normal basis. We have proved the theorem:

1. 10. THEOREM. *Let* $F/\boldsymbol{Q}$ *be a cyclic extension of prime degree* l *in which the prime* l *is unramified. Suppose the class number of the cyclotomic field* $\boldsymbol{Q}(l)$ *is one. Then every ambiguous ideal of* F *has a normal basis.*

In [5] we obtain a result by purely number-theoretic methods which includes 1. 10.

We give explicit normal bases for certain ideals of a cyclotomic field. Let $K = \boldsymbol{Q}(l)$, l an odd prime, ρ a primitive l-th root of unity, $\mathfrak{l}=(1-\rho)O_K$, $G = G(K/\boldsymbol{Q})$. For an ambiguous ideal $\mathfrak{A}$ of K, $\mathfrak{A} = [\alpha]$ if there exists $\alpha \in \mathfrak{A}$ such that every element of $\mathfrak{A}$ has the form $\sum_{\sigma \in G} a_\sigma \alpha^\sigma$, $a_\sigma \in \boldsymbol{Z}$. Clearly $O_K=[\rho]$ and $\mathfrak{l} = [1 - \rho]$. Set $m = (l-1)/2$ and fix a primitive root r mod l, i.e., $l-1$ is the smallest positive integer such that $r^{l-1} \equiv 1 \bmod l$. Let σ be the automorphism of K which takes $\rho \mapsto \rho^r$.

1. 11. PROPOSITION. (i) *The ideal* $\mathfrak{l}^m$ *of* $\boldsymbol{Q}(l)$ *has a normal basis*

$$\alpha = (1-\rho)(1-\rho^r)\cdots(1-\rho^{r^{m-1}}), \quad \textit{i.e.,} \quad \mathfrak{l}^m = [\alpha].$$

(ii) *For arbitrary* j, *if* $\mathfrak{l}^j = [\beta]$, *then* $\mathfrak{l}^{km+j} = [(\rho^\lambda \alpha)^k \beta]$, *for any* $k \in \boldsymbol{Z}$. λ *is defined (uniquely mod* l*) by* $\lambda(r-1) \equiv 1 \bmod l$. *If* S *denotes the normalized Gauss sum*

https://doi.org/10.1017/S0027763000024521 Published online by Cambridge University Press

$$S = \sum_{a=1}^{2m} \left(\frac{a}{l}\right) e^{2\pi i a/l}$$

and $\left(\frac{a}{l}\right)$ *the Legendre symbol, then* $\rho^\lambda \alpha = eS$, *where* $e = e(r, \rho) = \pm 1$.

Proof. (i) By induction we have

$$\alpha^{\sigma^j} = (-1)^j \rho^{-F_j} \alpha, \quad j = 1, 2, \cdots, l-1, \text{ and}$$
$$F_j = 1 + r + r^2 + \cdots + r^{j-1}.$$

Consider the set of elements $T = \{\alpha, \alpha^\sigma, \cdots, \alpha^{\sigma^{2m-1}}\}$. Since there are $2m+1$ distinct powers of ρ and at most $2m$ distinct elements in T, some power of ρ does not enter as a factor of α^{σ^j}. One checks that exactly one power ρ^λ of ρ does not appear. Of course exponents of ρ are considered mod l.

Thus

$$\begin{aligned}[\alpha] &= [\alpha, \cdots, \rho^{\lambda-1}\alpha, \rho^{\lambda+1}\alpha, \cdots, \rho^{2m}\alpha] \\ &= \alpha[1, \cdots, \rho^{\lambda-1}, \rho^{\lambda+1}, \cdots, \rho^{2m}] \\ &= \alpha \mathfrak{O}_K.\end{aligned}$$

But $\alpha = (1-\rho)^m E$, E unit of K. Therefore α generates a normal basis of $\mathfrak{l}^m$.

(ii) Consider $\rho^\lambda \alpha$. $(\rho^\lambda \alpha)^\sigma = -\rho^{\lambda r - 1}\alpha$. Thus $\lambda r - 1 \equiv \lambda \bmod l$ and $(\rho^\lambda \alpha)^\sigma = -\rho^\lambda \alpha$. It follows easily that $P = \rho^\lambda \alpha$ lies in the (unique) quadratic subfield of $\boldsymbol{Q}(l)$ and in fact $P^2 = (-1)^m l$. On the other hand if S denotes the normalized Gauss sum, then we know $S^2 = (-1)^m l$. Thus $P = eS$ for $e = e(r, \rho) = \pm 1$.

When $l = 5$, there are two primitive roots r mod 5. A computation shows $e(2, e^{2\pi i/5}) = +1$ and $e(3, e^{2\pi i/5}) = -1$. It is clear that P depends on the choice of ρ.

Now let M be the $\boldsymbol{Z}G$-module $[(\rho^\lambda \alpha)^k \beta] = [\gamma]$, $k \in \boldsymbol{Z}$. Recall

$$(\rho^\lambda \alpha)^\sigma = (-1)\rho^\lambda \alpha.$$

Thus

$$\begin{aligned}M &= [(\rho^\lambda \alpha)^k \beta, \ (-\rho^\lambda \alpha)^k \beta^\sigma, \cdots, (-\rho^\lambda \alpha)^k \beta^{\sigma^{l-2}}] \\ &= (\rho^\lambda \alpha)^k [\beta] \\ &= (1-\rho)^{km} E \cdot [\beta], \ E \text{ unit of } K, \\ &= \mathfrak{l}^{km+j}.\end{aligned}$$

https://doi.org/10.1017/S0027763000024521 Published online by Cambridge University Press

One can check that in $\boldsymbol{Q}(7)$, $\mathfrak{l}^2 = [(1-\rho)(1-\rho^3)]$; in $\boldsymbol{Q}(11)$, $\mathfrak{l}^2=[(1-\rho)(1-\rho^2)]$, $\mathfrak{l}^3 = [(1-\rho)(1-\rho^8)(1-\rho^9)]$. So we have shown up to but not including $\mathfrak{l}^4$ of $\boldsymbol{Q}(11)$ that $\mathfrak{l}^j$ $(j = 1, \cdots, l-2)$ has a normal basis of the form

$$\rho^{\mu}(1-\rho)(1-\rho^r)\cdots(1-\rho^{r^{j-1}}),\quad \mu \in \boldsymbol{Z},$$

r some primitive root mod l. However, this pattern fails for $\mathfrak{l}^4$ of $\boldsymbol{Q}(11)$.

Chapter II. Normal bases in wildly ramified Galois extensions

Let K/F be a Galois extension satisfying the conditions of the first paragraph of Chapter I. We may attach a subscript to an ideal to indicate the field in which it lies, e.g., $\mathfrak{A}_K$, $\mathfrak{A}_F$. A prime $\mathfrak{p}$ of F decomposes in K as $\mathfrak{p}O_K = (\mathfrak{P}_1 \cdots \mathfrak{P}_g)^e = \psi(\mathfrak{p})^e$, where $e = e_0 p^r$ ($e = e_0$ if characteristic of $O_F/\mathfrak{p}$ is zero), $(e_0, p) = 1$, and $r \geq 0$. K/F is *wildly ramified* (at $\mathfrak{P}_i$ or over $\mathfrak{p}$) if $r \geq 1$. Fix some $\mathfrak{P} = \mathfrak{P}_i$ dividing $\mathfrak{p}$. Let L be the fixed field of a subgroup H of $G = G(K/F)$. We have the ramification groups with respect to $\mathfrak{P}$ and K/L

$$V_i(\mathfrak{P}, K/L) = \{\sigma \in H \mid (\sigma - 1)O_K \subseteq \mathfrak{P}^{i+1}\},\quad i \geq 0.$$

When $L = F$, we abbreviate $V_i(\mathfrak{P}, K/F)$ as V_i. We write T for the inertia group V_0, V for V_1.

2.1. THEOREM. *Suppose K/F is wildly ramified. Let $\mathfrak{P}$ be any wildly ramified prime ideal of K over $\mathfrak{p}$ of F and $\mathfrak{A}$ an ambiguous ideal of K. The zero dimensional cohomology group $H^0(V, \mathfrak{A}) = 0$ implies* (i) *and* (ii). *If in addition the inertia group T is abelian, condition* (iii) *holds.*

(i) $\psi(\mathfrak{p})^s \| \mathfrak{A}$, *$s$ an integer, implies* $s \equiv 1 \bmod p^r$.

(ii) $V_2 = \{1\}$. *Hence* $V = \bigoplus_1^r \boldsymbol{Z}/p\boldsymbol{Z}$.

(iii) $T = V$.

Proof. $H^0(V, \mathfrak{A}) = 0$ means

$$S_{K/K_V}\mathfrak{A} = \mathfrak{A} \cap K_V,\quad K_V \text{ the fixed field of } V.$$

By 1.1 the exponent of $\mathfrak{P}_{K_V} = \mathfrak{P} \cap K_V$ in $S_{K/K_V}\mathfrak{A}$ is $[(m+s)/p^r]$ where $\mathfrak{P}^m \| \mathfrak{D}(K/K_V)$; the exponent of $\mathfrak{P}_{K_V}$ in $\mathfrak{A} \cap K_V$ is $[(p^r + s - 1)/p^r]$. Thus

$$[(m+s)/p^r] = [(p^r + s - 1)/p^r]. \tag{1}$$

For the remainder of the proof we consider s mod p^r; take $s \in \{1, 2, \cdots, p^r\}$.

https://doi.org/10.1017/S0027763000024521 Published online by Cambridge University Press

The ramification groups of K/K_V at $\mathfrak{P}$ are $V_i \cap G(K/K_V) = V_i \cap V$, $i \geq 0$. $(H:1)$ denotes the order of a subgroup H of G. We have

$$\begin{aligned} m &= \sum_{i=0}^{\infty} \{(V_i(\mathfrak{P}, K/K_V):1) - 1\} \\ &= \sum_i \{(V_i \cap V:1) - 1\} \\ &\geq 2\{(V:1) - 1\} = 2(p^r - 1). \end{aligned}$$

Equation (1) implies

$$[(2(p^r - 1) + s)/p^r] \leq 1 + [(s-1)/p^r]$$

or

$$[(s-1)/p^r] - [(s-2)/p^r] \geq 1.$$

For $s \in \{1, 2, \cdots, p^r\}$, s must be 1, i.e., $s \equiv 1 \bmod p^r$.

Assume $V_2 \neq \{1\}$, then

$$m \geq 2(p^r - 1) + (p - 1).$$

Using the result of (i), we have

$$[(2(p^r - 1) + (p-1) + 1)/p^r] \leq 1.$$

This is absurd, so $V_2 = \{1\}$. $V = \bigoplus_1^r \boldsymbol{Z}/p\boldsymbol{Z}$ since V_i/V_{i+1}, $i \geq 1$, is abelian of type $(p, p, \cdots, p)$.

We know that if $\sigma \in T$ and $\tau \in V_i$, $i \geq 1$, we have the commutator $\sigma\tau\sigma^{-1}\tau^{-1} \in V_{i+1}$ if and only if $\sigma^i \in V$ or $\tau \in V_{i+1}$. See Artin-Tate [1, Theorem 5, p. 111]. When T is abelian and $V_2 = \{1\}$, this yields $T = V$.

2. 2. *Remark.* If $\mathfrak{A}$ has a normal basis, it is cohomologically trivial. In particular, $H^0(V, \mathfrak{A}) = 0$.

2. 3. We determine the ideals with normal bases in wildly ramified abelian extensions $K/\boldsymbol{Q}$. For $h \geq 1$, let $L_h(l)$ denote the unique subfield of $\boldsymbol{Q}(l^{h+1})$ of degree l^h where l is a prime. If $l = 2$, we see $L_h(l) = \boldsymbol{Q}(2^{h+1})$. Let $L_1(l) = L(l)$. Define the rational integer D' as the product of all the rational primes which are wildly ramified in the extension K.

Suppose $K/\boldsymbol{Q}$ is a wildly ramified abelian extension. Then $K \subseteq \Omega$, where

$$\Omega = P \cdot \prod_{l \mid D'} L_h(l).$$

https://doi.org/10.1017/S0027763000024521 Published online by Cambridge University Press

Of course h depends on l; $P/\boldsymbol{Q}$ is a tamely ramified abelian extension. In the remainder of this chapter we use the notation $G = G(\Omega/\boldsymbol{Q})$ and the subgroups A and B of G fix the fields Ω' and K respectively.

DEFINITION. The Galois extension $K/\boldsymbol{Q}$ satisfies hypothesis $H(p)$ if, for a prime $\mathfrak{P}$ of K dividing the rational prime p,

$$V_0(\mathfrak{P}, K/\boldsymbol{Q}) = V_1(\mathfrak{P}, K/\boldsymbol{Q}) = \bigoplus_1^r \boldsymbol{Z}/p\boldsymbol{Z}, \quad r \geq 1, \quad \text{and} \quad V_2(\mathfrak{P}, K/\boldsymbol{Q}) = \{1\}.$$

2. 4. Suppose $K \subseteq \Omega$ described in 2. 3 and K satisfies $H(l)$, l an odd prime. Set

$$M = P \cdot \prod_{\substack{p \mid D' \\ p \neq l}} L_h(p), \quad \Omega' = M \cdot L(l).$$

We claim $K \subseteq \Omega'$. Let $\mathfrak{L}$ be a prime divisor of l in Ω. Since l is totally ramified in $L_h(l)$ and tamely ramified in M, we have $M \cap L_h(l) = \boldsymbol{Q}$. Hence the order of $V = V_1(\mathfrak{L}, \Omega/\boldsymbol{Q})$ is l^h. For any subgroup $H \subseteq G$ put $\Omega_H =$ the subfield of Ω fixed by elements of H. Since l is tamely ramified in M, $\Omega_V \supseteq M$; also $[\Omega : M] = [L_h(l) : \boldsymbol{Q}] = l^h$. Hence $\Omega_V = M$ and V is cyclic. This and hypothesis $H(l)$ imply the ramification index of l in K is l. Hence $V \cap B = V_1(\mathfrak{L}, \Omega/K)$ has order l^{h-1}. Thus $A \subseteq B$, which implies $K \subseteq \Omega'$.

Suppose K satisfies $H(l)$, l odd, and $K \subseteq P \cdot M = \Omega$, where

$$M = L(l) \cdot \prod_{\substack{p \mid D' \\ p \neq l}} L_h(p).$$

We may assume l is unramified in P. In fact let P' be the inertia field of $\mathfrak{L}_P \mid l$ relative to $P/\boldsymbol{Q}$. The prime l is unramified in P' and $\mathfrak{L}_{P'}$ is totally ramified in P. We claim $K \subseteq P' \cdot M$, which we now call Ω'. Let $M'' \neq \boldsymbol{Q}$ be a subfield of M. In M'' some prime ramifies wildly, so $M'' \not\subseteq P$. Therefore $P \cap M = \boldsymbol{Q}$. Set

$$M' = \prod_{\substack{p \mid D' \\ p \neq l}} L_h(p)$$

and $P'M' = P_0$. Note that P_0 is the inertia field of $\mathfrak{L}_\Omega \mid l$ relative to $\Omega/\boldsymbol{Q}$, since l is unramified in $P_0 = P'M'$ and $\mathfrak{L}_{P_0}$ is totally ramified in Ω. Let T be the inertia group of $\mathfrak{L}_\Omega$ fixing P_0. T is an abelian group of order al, where $l = (T : A)$, $a = (A : 1) = [\Omega : \Omega'] = [P : P']$. Since $P/\boldsymbol{Q}$ is tamely ramified, $(l, a) = 1$. Thus $T = \boldsymbol{Z}/l\boldsymbol{Z} \oplus A$. Since the ramification index of l in K is l

https://doi.org/10.1017/S0027763000024521 Published online by Cambridge University Press

$T \cap B$ has order a. But T has exactly one subgroup of order a implies $T \cap B = A$, $A \subseteq B$, and finally $K \subseteq \Omega'$.

2.5. Suppose K satisfies $H(2)$ and $K \subseteq L_{h+1}(2) \cdot M = \Omega$, where $h \geq 1$ and $M/\boldsymbol{Q}$ is abelian and unramified over the prime 2. We claim $K \subseteq L(2) \cdot M = \Omega'$. Let $\mathfrak{P}$ be a prime of Ω dividing 2. Since $M \cap L_{h+1}(2) = \boldsymbol{Q}$, $G(L_{h+1}(2)/\boldsymbol{Q}) \cong G(\Omega/M)$. $\Omega_V = M$ as above. Since

$$T = V = V_1(\mathfrak{P}, \Omega/\boldsymbol{Q}) = \boldsymbol{Z}/2\boldsymbol{Z} \oplus \boldsymbol{Z}/2^h\boldsymbol{Z}$$

and hypothesis $H(2)$ holds, the ramification index of 2 in K is 2 or 4. Consider the latter case. If a prime $\mathfrak{P}_K | 2$, then $\mathfrak{P}_K^6 \| \mathfrak{D}(K/\boldsymbol{Q})$; $\mathfrak{P}^m \| \mathfrak{D}(\Omega/\boldsymbol{Q})$, $m = (h+1)2^{h+1}$. Consequently, if $\mathfrak{P}^x \| \mathfrak{D}(\Omega/K)$, we have by the chain rule for differents

$$(h+1)2^{h+1} = 6 \cdot 2^{h-1} + x. \tag{2}$$

By the theorem on the bound of the power of $\mathfrak{P}$ dividing $\mathfrak{D}(\Omega/K)$, e.g., Weiss [10, Prop. 3-7-23]

$$x \leq (h-1)2^{h+1} + 2^{h-1} - 1. \tag{3}$$

Equations (2) and (3) cannot both hold. Hence the ramification index of 2 in K is 2.

$L_{h+1}(2)$ has three subfields of degree 2, namely $L(2) = \boldsymbol{Q}(\sqrt{-1})$ and $\boldsymbol{Q}(\sqrt{\pm 2})$. Since the ramification index of 2 in K is 2, the subgroup $V \cap B$ has order 2^h. V contains the subgroup A fixing Ω' of order 2^h. Either $B \supseteq A$ (in which case $K \subseteq \Omega'$) or B contains one of the two subgroups fixing the field $M(\sqrt{\pm 2})$.

We assume $K \subseteq M(\sqrt{2})$ and obtain a contradiction. Let F be the ramification subfield of K, so $[K: F] = 2$. Since $V_2(\mathfrak{P}_K, K/\boldsymbol{Q}) = \{1\}$, $K \neq F(\sqrt{2})$. Since $\mathfrak{P}_F^3 \| D(F(\sqrt{2})/F)$ and $\mathfrak{P}_F^2 \| D(K/F)$, where in each case D denotes the relative discriminant, it follows that the ramification index of 2 in $K(\sqrt{2})$ is 4. But by assumption K and hence $K(\sqrt{2}) \subseteq$ the field $M(\sqrt{2})$ in which the ramification index of 2 is 2. Of course we could have replaced $\sqrt{2}$ by $\sqrt{-2}$. Thus $K \subseteq L(2) \cdot M$ as claimed. Sections 2.4 and 2.5 give the following theorem.

2.6. THEOREM. *Assume $K/\boldsymbol{Q}$ abelian and at each rational prime l wildly ramified in K we have K satisfies hypothesis $H(l)$. Then*

https://doi.org/10.1017/S0027763000024521 Published online by Cambridge University Press

(i) $$K \subseteq \Omega = P \cdot \prod_{l|D'} L(l)$$

where $P/\boldsymbol{Q}$ is abelian and tamely ramified and the absolute discriminant of P is prime to D'.

(ii) *An ambiguous ideal $\mathfrak{A}$ of K has a normal basis implies that at each rational prime l wildly ramified in K we have $\psi(l)^s \| \mathfrak{A}$ where $s \equiv 1 \bmod l$ and for a prime $\mathfrak{P}$ of K dividing l we have*

$$V_0(\mathfrak{P}, K/\boldsymbol{Q}) = V_1(\mathfrak{P}, K/\boldsymbol{Q}) = \boldsymbol{Z}/l\boldsymbol{Z}$$

and

$$V_2(\mathfrak{P}, K/\boldsymbol{Q}) = \{1\}.$$

The following proposition provides explicit normal bases.

2.7. PROPOSITION. *Let l be an odd prime, $L = L_1(l)$. Then*

(i) *L is the only wildly ramified subfield of $\boldsymbol{Q}(l^{h+1})$ containing ideals with normal bases.*

(ii) *If the prime ideal $\mathfrak{L} | l$, $\mathfrak{L}$ of L, then $\mathfrak{L}$ has a normal basis. Explicitly, $\mathfrak{L} = [1 + T]$, where $T = \mathrm{S}(\rho)$, S = the trace function from $\boldsymbol{Q}(l^2)$ to L, ρ a primitive l^2 root of unity. $\mathfrak{L}$ is the only primitive ambiguous ideal of L with a normal basis.*

(iii) *$\boldsymbol{Q}(\sqrt{-1})$ is the only (wildly ramified) subfield of $\boldsymbol{Q}(2^{h+1})$ containing ideals with normal bases. If $\mathfrak{L} | 2$, $\mathfrak{L}$ a prime ideal of $\boldsymbol{Q}(\sqrt{-1})$, then $\mathfrak{L} = [1 + \sqrt{-1}]$ is the only primitive ambiguous ideal of $\boldsymbol{Q}(\sqrt{-1})$ with a normal basis.*

Proof. Parts (i)–(iii) of 2.1 imply that the ideal $\mathfrak{L}$ of L is the only candidate for a primitive ambiguous ideal of a wildly ramified subfield of $\boldsymbol{Q}(l^{h+1})$, l odd, to have a normal basis.

Every element of $\mathrm{O}_{\boldsymbol{Q}(l^2)}$ may be written (not uniquely) as $\sum_{i=1}^{l^2-1} a_i \rho^i$, $a_i \in \boldsymbol{Z}$. Since $\boldsymbol{Q}(l^2)/L$ is tamely ramified, $\mathrm{SO}_{\boldsymbol{Q}(l^2)} = \mathrm{O}_L$. Therefore $W = \{\mathrm{S}(\rho^j) \mid j = 1, \cdots, l^2 - 1\}$ contains a $\boldsymbol{Z}$-basis of O_L. Let r be a primitive root mod l^2, $G(\boldsymbol{Q}(l^2)/\boldsymbol{Q}) = \langle \sigma \rangle$, $\rho^\sigma = \rho^r$, and $T_i = \mathrm{S}(\rho^{r^i})$, $i = 0, \cdots, l(l-1) - 1$. Note that

$$T_i = \mathrm{S}(\rho^{r^i}) = \mathrm{S}(\rho^{\sigma^i}) = \mathrm{S}(\rho)^{\sigma^i} = \mathrm{S}(\rho)^{\sigma^j} = T_j$$

for $i \equiv j \bmod l$. Also $\mathrm{S}(\rho^{il}) = -1$ for $i = 1, \cdots, l-1$. Thus

$$W = \{-1, T_0, \cdots, T_{l-1}\}.$$

https://doi.org/10.1017/S0027763000024521 Published online by Cambridge University Press

But $T_0 + \cdots + T_{l-1} =$ sum primitive l^2 roots of unity $= 0$. Thus O_L has a $\boldsymbol{Z}$-basis consisting of the elements $1, T_0, \cdots, T_{l-2}$.

Set $T = T_0$. If $\mathfrak{L} | l$ in L, then $1 + T$ generates a normal basis of $\mathfrak{L}$. In fact, $\rho - 1$ generates the principal ideal of $\boldsymbol{Q}(l^2)$ dividing l and

$$S(\rho - 1) = T - (l - 1) \in \mathfrak{L}.$$

Therefore $M = [1 + T] \subseteq \mathfrak{L}$. It suffices to show that the index of M in O_L as a $\boldsymbol{Z}$-module is l.

$$[O_L : M] = \begin{vmatrix} 1 & 1 & 0 & 0 & \cdots & 0 \\ 1 & 0 & 1 & 0 & \cdots & 0 \\ & & & \cdots & & \\ 1 & 0 & 0 & 0 & \cdots & 1 \\ 1 & -1 & -1 & -1 & \cdots & -1 \end{vmatrix}_{l \times l} = l \ .$$

The proof of (iii) follows that of (i) and (ii).

2. 8. THEOREM. *Let $\mathfrak{A}$ be an ambiguous ideal of K. Suppose*

$$K = \prod_{l | D'} L(l)$$

and at each wildly ramified prime l of K including $l = 2$, $\phi(l)^s \| \mathfrak{A}$, $s \equiv 1 \bmod l$; then $\mathfrak{A}$ has a $K/\boldsymbol{Q}$-normal basis.

Proof. By the remark of 1. 7 it suffices to consider $\mathfrak{A}$ a primitive ambiguous ideal. For any Galois extension M of $\boldsymbol{Q}$ and rational prime l define $\phi(l, M)$ to be the product of all distinct prime ideals of M dividing l. Any primitive ambiguous ideal $\mathfrak{A}$ of K with a normal basis must have the form

$$\mathfrak{A} = \prod_{l | D'} \phi(l, K).$$

The ideals $\phi(l, L(l))$ have normal bases in their respective fields. The extension $K/L(l)$ is unramified over the prime of $L(l)$ dividing l, hence

$$\phi(l, L(l))O_K = \phi(l, K).$$

The absolute discriminants of the fields $L(l)$ are pairwise coprime, hence we may "multiply the normal bases" (see 1. 8) to get a $K/\boldsymbol{Q}$-normal basis of $\mathfrak{A}$.

https://doi.org/10.1017/S0027763000024521 Published online by Cambridge University Press

References

[1] E. Artin and J. Tate, *Class field theory*, Harvard (1961).
[2] P.G.L. Dirichlet and R. Dedekind, *Vorlesungen über Zahlentheorie*, 4th ed., supplement 11, Friedr. Vieweg und Sohn (1894).
[3] A. Fröhlich, *The module structure of Kummer extensions over Dedekind domains*, J. reine angew. Math. **209** (1962), 39–53.
[4] D. Hilbert, *Gesammelte Abhandlungen*, vol. 1, Chelsea (1965). (*Die Theorie der algebraischen Zahlkörper*, Jahresber. der Deutsch. Math. Ver. **4** (1897), 175–546).
[5] S. Kuroda and S. Ullom, *Root numbers associated with normal bases* (in preparation).
[6] H-W. Leopoldt, *Über die Hauptordnung der ganzen Elemente eines abelschen Zahlkörpers*, J. reine angew. Math. **201** (1959), 119–149.
[7] E. Noether, *Normalbasis bei Körpern ohne höhere Verzweigung*, J. reine angew. Math. **167** (1931), 147–152.
[8] D.S. Rim, *Modules over finite groups*, Ann. of Math. **69** (1959), 700–712.
[9] A. Speiser, *Gruppendeterminante und Körperdiskriminante*, Math. Ann. **77** (1916), 546–562.
[10] E. Weiss, *Algebraic number theory*, McGraw-Hill (1963).
[11] H. Yokoi, *On the ring of integers in an algebraic number field as a representation module of Galois group*, Nagoya Math. J. **16** (1960), 83–90.
[12] H. Yokoi, *A cohomological investigation of the discriminant of a normal algebraic number field*, Nagoya Math. J. **27** (1966), 207–211.

University of Maryland
College Park, Maryland

https://doi.org/10.1017/S0027763000024521 Published online by Cambridge University Press