CYCLIC EXTENSIONS WITHOUT RELATIVE INTEGRAL BASES

LEON R. McCULLOH

Let K be an algebraic number field and $\mathfrak{o}$ the ring of algebraic integers in K. If $\mathfrak{o}$ is a principal ideal domain (p.i.d.) then any finite extension Λ/K has an integral basis over $\mathfrak{o}$ (i.e., the ring of integers $\mathfrak{O}=\mathfrak{O}(\Lambda)$ of Λ is a free $\mathfrak{o}$-module). The converse of this was shown by Mann [5]. More precisely, he proved that if $\mathfrak{o}$ is not a p.i.d., there is a quadratic extension Λ/K which has no integral basis over $\mathfrak{o}$. Thus $\mathfrak{o}$ is a p.i.d. if and only if every quadratic extension of K has an integral basis. One can also show ([7] or the corollary below) that if K contains a primitive cube root of 1, then $\mathfrak{o}$ is a p.i.d. if and only if every cyclic extension of degree 3 has an integral basis. However, the analogous theorem with 3 replaced by a prime $p>3$ is false.

The problem considered here is the following. Given a finite group G of order n and an algebraic number field K, consider all normal extensions Λ/K with Galois group isomorphic to G. What are the $\mathfrak{o}$-module types of the $\mathfrak{O}(\Lambda)$ for these extensions? In particular, when are all the $\mathfrak{O}(\Lambda)$ free? In Theorems 1 and 2 we answer these questions in the case that G is cyclic of order n and K contains the nth roots of unity.

A finitely generated torsion free $\mathfrak{o}$-module M of a given $\mathfrak{o}$-rank is characterized by its Steinitz class $C(M)=C_{\mathfrak{o}}(M)$ which is an $\mathfrak{o}$-ideal class of K. Specifically, $M\cong\mathfrak{o}^{(r-1)}\oplus J$ where r is the $\mathfrak{o}$-rank of M, $\mathfrak{o}^{(r-1)}$ is a free $\mathfrak{o}$-module of rank $r-1$, and J is any ideal in the class $C(M)$. If Λ/K is a finite extension, let $\mathfrak{D}=\mathfrak{D}(\mathfrak{O}(\Lambda)/\mathfrak{o})$ be the discriminant ideal and let $\Delta=\Delta(\Lambda/K)$ be the discriminant of a basis of Λ/K. It was shown by Artin that the ideal $(\mathfrak{D}/(\Delta))^{1/2}$ is an $\mathfrak{o}$-ideal lying in $C_{\mathfrak{o}}(\mathfrak{O}(\Lambda))$. (For proofs of the above remarks, see Artin [1] or Fröhlich [2] and [3].)

DEFINITION. If l is an odd prime, let $d(l)=(l-1)/2$, and let $d(2)=1$. We define, for any integer n, $d(n)=\text{g.c.d. }\{d(l)\mid l \text{ is a prime divisor of } n\}$.

THEOREM 1. *Let Λ/K be normal of degree n. Then $C_{\mathfrak{o}}(\mathfrak{O}(\Lambda))$ is a $d(n)$th power in the ideal class group of $\mathfrak{o}$.*

PROOF. If n is even, $d(n)=1$ and the theorem is trivial. If n is odd,

Presented to the Society, April 23, 1966; received by the editors February 17, 1966.

the discriminant Δ of any basis of Λ/K is a square in K, so $C(\mathfrak{O})$ is the class of $\mathfrak{D}^{1/2}$. Let $\mathfrak{p}$ be any prime of $\mathfrak{o}$ and suppose $\mathfrak{p}\cdot\mathfrak{O}=(\mathfrak{P}_1\cdots\mathfrak{P}_g)^e$ where each prime $\mathfrak{P}_j$ is of degree f over $\mathfrak{p}$. Let G_i $(i=0,\cdots,\nu)$ be the ramification groups of $\mathfrak{P}_1$. Then, by the Hilbert formula, $\mathfrak{D}$ is exactly divisible by $\mathfrak{p}^r$ where $r=fg\cdot\sum\{(\#(G_i)-1)\mid i=0,\cdots,\nu\}$. Clearly $2d(n)\mid(\#(G_i)-1)$ for each i, so $d(n)\mid(r/2)$.

THEOREM 2. *Let n be a positive integer and let $\zeta\in K$ where ζ is a primitive nth root of* 1. *If $\mathfrak{c}$ is any $\mathfrak{o}$-ideal class of K, there is a cyclic extension Λ/K of degree n with $C_0(\mathfrak{O}(\Lambda))=\mathfrak{c}^{d(n)}$. (In fact, there are infinitely many such extensions, and they may be chosen so that $\mathfrak{D}(\mathfrak{O}(\Lambda)/\mathfrak{o})$ is relatively prime to any preassigned $\mathfrak{o}$-ideal $\mathfrak{b}$ of K.)*

The following is an immediate consequence.

COROLLARY. (*Same hypothesis.*) *$\mathfrak{O}(\Lambda)$ is a free $\mathfrak{o}$-module for every cyclic extension Λ/K of degree n if and only if $d(n)$ is divisible by the exponent of the ideal class group of $\mathfrak{o}$.*

PROOF OF THEOREM 2. We prove the theorem first for the case $n=l^r$ where l is a prime. If $\mathfrak{m}$ is any ideal in $\mathfrak{o}$, there are infinitely many prime ideals in any ideal class mod $\mathfrak{m}$. (The ideal class group mod $\mathfrak{m}$ is the quotient of the group of all $\mathfrak{o}$-ideals prime to $\mathfrak{m}$ modulo the subgroup of principal ideals of form $\alpha\cdot\mathfrak{o}$ where $\alpha\equiv 1 \pmod{\mathfrak{m}}$.)

First suppose l is odd. Let $\mathfrak{c}$ be any ideal class and let $t>1$ be any integer such that $\mathfrak{c}^t=\mathfrak{c}$. (We may suppose t is odd.) Let $\mathfrak{p}$ be any prime ideal in $\mathfrak{c}$ such that $\mathfrak{p}\nmid l$. Choose distinct primes $\mathfrak{p}_1,\cdots,\mathfrak{p}_t$ in the same ideal class mod $\mathfrak{m}$ as $\mathfrak{p}$, where we take $\mathfrak{m}=(1-\zeta)^{l^{2r}}$. Then choose primes $\mathfrak{q}_1,\cdots,\mathfrak{q}_t$ in the inverse ideal class of $\mathfrak{p}$ mod $\mathfrak{m}$. Then choose positive integers $a_1,\cdots,a_t$, prime to l, such that $\sum a_i=lt$. (For example, $a_i=l-1$ for $1\leqq i\leqq(t-1)/2$, $a_i=l+1$ for $(t+1)/2\leqq i\leqq t-1$, and $a_t=l+2$.) Then $(\prod_{i=1}^t\mathfrak{p}_i^{a_i})\cdot(\prod_{i=1}^t\mathfrak{q}_i)^l=\mu\cdot\mathfrak{o}$, a principal ideal where $\mu\equiv 1 \pmod{\mathfrak{m}}$. If α is a root of $f(x)=X^{l^r}-\mu$, then $\Lambda=K(\alpha)$ is a cyclic extension of K of degree l^r. We show that $C(\mathfrak{O}(\Lambda))=\mathfrak{c}^{(l-1)/2}$. To do this, we must compute $\mathfrak{D}(\mathfrak{O}(\Lambda)/\mathfrak{o})$.

First we show that no higher (i.e., wild) ramification occurs. For let $\mathfrak{l}$ be a prime of K dividing l, and suppose $\mathfrak{l}^a$ exactly divides $(1-\zeta)$. Let $\mathfrak{L}$ be a prime of Λ dividing $\mathfrak{l}$, say $\mathfrak{L}^b$ exactly divides $\mathfrak{l}$. Now, $1-\mu=\prod_\sigma(1-\sigma(\alpha))$ where σ runs over the Galois group G of Λ/K. Since $1-\mu$ is divisible by $\mathfrak{m}=(1-\zeta)^{l^{2r}}$, at least one of the factors (which we may take to be $(1-\alpha)$) is divisible at least by $\mathfrak{L}^{abl^r}$. But, for any $\sigma\in G$, $\sigma\neq 1$, we have $\sigma(\alpha)-\alpha=(\zeta^j-1)\alpha$ for some $0<j<l^r$. Since $\mathfrak{L}\nmid\alpha$ and $(\zeta^j-1)\mid(\zeta^{l^{r-1}}-1)$ which is exactly divisible by $\mathfrak{L}^{abl^{r-1}}$, we have $\sigma(\alpha)-\alpha$ divisible at most by $\mathfrak{L}^{abl^{r-1}}$. Hence, in the $\mathfrak{L}$-adic

metric on Λ, α is closer to 1 than to any of its conjugates $\sigma(\alpha)$. Then, by Krasner's Lemma (see, e.g., [8, p. 82]), letting K^* and Λ^* denote the completions of K and Λ at $\mathfrak{L}$, we have $\Lambda^* = K^*(\alpha) \subseteq K^*(1) = K^*$. Hence, $\mathfrak{L}$ is unramified over K and, indeed, of degree 1 over K.

Since $f'(\alpha) = l^r(\alpha)^{l^r-1}$, the only possible divisors of $\mathfrak{D}$ are the divisors of μ. Clearly $\mathfrak{p}_1, \cdots, \mathfrak{p}_t$ are completely ramified in Λ so that $\mathfrak{D}$ is exactly divisible by $\mathfrak{p}_i^{l^r-1}$. On the other hand, it is easily seen that the inertial field for any prime divisor of $\mathfrak{q}_j$ $(1 \leqq j \leqq t)$ is $K((\mu)^{1/l}) = K(\alpha^{l^{r-1}})$. (To see this: $\mathfrak{q}_i$ is unramified in $K((\mu)^{1/l})$, for we can easily find $\mu' = \beta^l \mu$ where $\mathfrak{q}_j$ is prime to μ' and $K((\mu)^{1/l}) = K((\mu')^{1/l})$. Also, clearly, the ramification index of any divisor of $\mathfrak{q}_j$ in Λ is at least l^{r-1}, whence it is exactly l^{r-1}.) Thus, $\mathfrak{D}$ is exactly divisible by $\mathfrak{q}_j^{l(l^{r-1}-1)} = q_j^{l^r-l}$. Hence,

$$\mathfrak{D}^{1/2} = \left(\prod_{i=1}^{t} \mathfrak{p}_i\right)^{(l^r-1)/2} \left(\prod_{j=1}^{t} \mathfrak{q}_j\right)^{(l^r-l)/2} \sim \mathfrak{p}^{-t(l^r-1)/2}\mathfrak{p}^{t(l^r-l)/2}$$

$$= \mathfrak{p}^{t(l-1)/2} \sim \mathfrak{p}^{(l-1)/2}.$$

(Here, $\sim$ means "belongs to the same ideal class as.") Hence $C(\mathfrak{O}(\Lambda)) = \mathfrak{c}^{(l-1)/2}$.

The case $l=2$ is similar. Choose a prime $\mathfrak{p} \nmid 2$ in the class $\mathfrak{c}$. Take primes $\mathfrak{p}_1$ and $\mathfrak{p}_3$ in the same class mod $\mathfrak{m}$ as $\mathfrak{p}$, and take $\mathfrak{p}_2$ in the class of $\mathfrak{p}^{-2}$ mod $\mathfrak{m}$, where $\mathfrak{m}$ is a power of 2 large enough to avoid higher ramification. Then $\mathfrak{p}_1\mathfrak{p}_2^2\mathfrak{p}_2^3 = (\mu)$ where $\mu \equiv 1$ (mod $\mathfrak{m}$). Let α be a root of $f(x) = x^{2^r} - \mu$ and consider $\Lambda = K(\alpha)$. Then $\mathfrak{D} = (\mathfrak{p}_1\mathfrak{p}_3)^{2^r-1}\mathfrak{p}_2^{2^r-2}$. Also, $f'(\alpha) = 2^r \cdot \alpha^{2^r-1}$, so if Δ is the discriminant of the basis $1, \alpha, \alpha^2, \cdots, \alpha^{2^r-1}$, then $(\Delta) = (2^r)^{2^r}(\mu)^{2^r-1}\,\mathfrak{o}$. Hence $((\mathfrak{D}/\Delta)^{1/2}) \sim \mathfrak{p}_3^{-(2^r-1)}\mathfrak{p}_2^{-2^{r-1}} \sim (\mathfrak{p}^{1-2^r})\mathfrak{p}^{2^r} = \mathfrak{p}$. Hence $C(\mathfrak{O}(\Lambda)) = \mathfrak{c}$. This completes the proof of Theorem 2 for the case $n = l^r$.

Before proving the general case, we prove the following lemma. (This is well known, but it seems to be hard to find in print. Compare [4, p. 202] and [6, p. 72]).

LEMMA. *Let Λ_1 and Λ_2 be linearly disjoint over K (i.e. $\Lambda_1 \cdot \Lambda_2 \cong \Lambda_1 \otimes_K \Lambda_2$). Let $\mathfrak{O}_i = \mathfrak{O}(\Lambda_i)$. If $\mathfrak{D}(\mathfrak{O}_1/\mathfrak{o})$ and $\mathfrak{D}(\mathfrak{O}_2/\mathfrak{o})$ are relatively prime, then the maximal $\mathfrak{o}$-order of $\Lambda_1 \otimes_K \Lambda_2$ is $\mathfrak{O}_1 \otimes_{\mathfrak{o}} \mathfrak{O}_2$ and its discriminant over $\mathfrak{o}$ is $\mathfrak{D}(\mathfrak{O}_1/\mathfrak{o})^{[\Lambda_2:K]}\mathfrak{D}(\mathfrak{O}_2/\mathfrak{o})^{[\Lambda_1:K]}$.*

PROOF. Let $\mathfrak{O}'$ be the maximal $\mathfrak{o}$-order of $\Lambda_1 \otimes_K \Lambda_2$. Then $\mathfrak{O}' \supseteq \mathfrak{O}_1 \otimes_{\mathfrak{o}} \mathfrak{O}_2$, and $\mathfrak{D}(\mathfrak{O}_1 \otimes_{\mathfrak{o}} \mathfrak{O}_2/\mathfrak{O}_2) = \mathfrak{D}(\mathfrak{O}'/\mathfrak{O}_2)[\mathfrak{O}' : \mathfrak{O}_1 \otimes_{\mathfrak{o}} \mathfrak{O}_2]^2$ where the notation $[M:N]$ denotes the module index (see Fröhlich [2], [3] and [4]). Also,

$$\mathfrak{D}(\mathfrak{O}'/\mathfrak{o}) = N_{\Lambda_i/K}(\mathfrak{D}(\mathfrak{O}'/\mathfrak{O}_i)) \cdot \mathfrak{D}(\mathfrak{O}_i/\mathfrak{o})^{[\Lambda_j:K]} \tag{1}$$

where the pair (i, j) is $(1, 2)$ or $(2, 1)$.

Now, since $\mathfrak{D}(\mathfrak{O}'/\mathfrak{O}_i)$ divides $\mathfrak{D}(\mathfrak{O}_1\otimes\mathfrak{O}_2/\mathfrak{O}_i)=\mathfrak{D}(\mathfrak{O}_j/\mathfrak{o})\cdot\mathfrak{O}_i$, $N_{\Lambda_i/K}(\mathfrak{D}(\mathfrak{O}'/\mathfrak{O}_i))$ divides $\mathfrak{D}(\mathfrak{O}_i/\mathfrak{o})^{[\Lambda_i/K]}$ and is, therefore, prime to $\mathfrak{D}(\mathfrak{O}_i/\mathfrak{o})$. Hence, from (1) we have $N_{\Lambda_i/K}(\mathfrak{D}(\mathfrak{O}'/\mathfrak{O}_i))=(\mathfrak{D}(\mathfrak{O}_j/\mathfrak{o})^{[\Lambda_i/K]}$ and $\mathfrak{D}(\mathfrak{O}'/\mathfrak{O}_i)=\mathfrak{D}(\mathfrak{O}_1\otimes\mathfrak{O}_2/\mathfrak{O}_i)$ whence $[\mathfrak{O}':\mathfrak{O}_1\otimes\mathfrak{O}_2]=(1)$ and $\mathfrak{O}'=\mathfrak{O}_1\otimes\mathfrak{O}_2$.

We next prove Theorem 2 in the general case. Let $n=\prod_{i=1}^{s} l_i^{r_i}$ where the l_i are distinct primes. Let $d=d(n)$. For each i, let $d(l_i)=d\cdot h_i$. Then g.c.d. $\{h_i \mid 1\leqq i\leqq s\}=1$ and $(h_i, l_i)=1$. Hence g.c.d. $\{h_i n/l_i^{r_i} \mid 1\leqq i\leqq s\}=1$. For, suppose to the contrary that the prime p is a common divisor. We may suppose $p\nmid h_1$ whence $p \mid (n/l_1^{r_1})$ so $p=l_2$, say. But then $p\nmid (h_2 n/l_2^{r_2})$.

Choose integers x_i such that $\sum\{x_i h_i n/l_i^{r_i} \mid 1\leqq i\leqq s\}=1$. Then $d=\sum\{x_i d(l_i)n/l_i^{r_i} \mid 1\leqq i\leqq s\}$. Choose cyclic extensions Λ_i/K of degree $l_i^{r_i}$ having $C(\mathfrak{O}(\Lambda_i))=\mathfrak{c}^{x_i d(l_i)}$ and such that the $\mathfrak{D}(\mathfrak{O}(\Lambda_i)/\mathfrak{o})$ are relatively prime in pairs. Then $\Lambda=\Lambda_1\cdots\Lambda_s\cong\Lambda_1\otimes_K\cdots\otimes_K\Lambda_s$ and the maximal order $\mathfrak{O}(\Lambda)\cong\mathfrak{O}(\Lambda_1)\otimes\cdots\otimes\mathfrak{O}(\Lambda_s)$. Hence (see Fröhlich [3, p. 32])

$$C(\mathfrak{O}(\Lambda)) = \prod\left\{C(\mathfrak{O}(\Lambda_i))^{n/l_i^{r_i}} \,\middle|\, 1 \leqq i \leqq s\right\} = \mathfrak{c}^d.$$

References

1. E. Artin, *Questions de base minimale dans la théorie des nombres algébriques*, Colloques Internationaux du Centre National de la Récherche Scientifique, No. XXIV, pp. 19–20, Paris, 1950.

2. A. Fröhlich, *Discriminants of algebraic number fields*, Math. Z. **74** (1960), 18–28.

3. ———, *Ideals in an extension field as modules over the algebraic integers in a finite number field*, Math. Z. **74** (1960), 29–38.

4. ———, *Invariants for modules over commutative separable orders*, Quart. J. Math. Oxford Ser. **16** (1965), 193–232.

5. H. B. Mann, *On integral bases*, Proc. Amer. Math. Soc. **9** (1958), 167–172.

6. ———, *Introduction to algebraic number theory*, The Ohio State University Press, Columbus, 1955.

7. L. R. McCulloh, *Integral bases in Kummer extensions of Dedekind fields*, Canad. J. Math. **15** (1963), 755–765.

8. E. Weiss, *Algebraic number theory*, McGraw-Hill, New York, 1963.

University of Illinois