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 $\Lambda/K$ has an integral basis over $\mathfrak{o}$ (i.e., the ring of integers $\mathcal{O} = \mathcal{O}(\Lambda)$ of $\Lambda$ 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 $\Lambda/K$ 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 $\Lambda/K$ with Galois group isomorphic to $G$. What are the $\mathfrak{o}$-module types of the $\mathcal{O}(\Lambda)$ for these extensions? In particular, when are all the $\mathcal{O}(\Lambda)$ free? In Theorems 1 and 2 we answer these questions in the case that $G$ is cyclic of order $n$ and $K$ contains the $n$th 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 $\Lambda/K$ is a finite extension, let $\mathcal{D} = \mathcal{D}(\mathcal{O}(\Lambda)/\mathfrak{o})$ be the discriminant ideal and let $\Delta = \Delta(\Lambda/K)$ be the discriminant of a basis of $\Lambda/K$. It was shown by Artin that the ideal $(\mathcal{D}/(\Delta))^{1/2}$ is an $\mathfrak{o}$-ideal lying in $C_\mathfrak{o}(\mathcal{O}(\Lambda))$. (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 $n$, $d(n) = \gcd(d(l) | l$ is a prime divisor of $n$).

**Theorem 1.** Let $\Lambda/K$ be normal of degree $n$. Then $C_\mathfrak{o}(\mathcal{O}(\Lambda))$ 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,
the discriminant $\Delta$ of any basis of $\Delta/K$ is a square in $K$, so $C(\mathcal{O})$ is the class of $\mathcal{D}^{1/2}$. Let $p$ be any prime of $\mathfrak{o}$ and suppose $p \cdot \mathcal{O} = (\mathfrak{B}_1 \cdots \mathfrak{B}_q)^*$ where each prime $\mathfrak{B}_i$ is of degree $f$ over $p$. Let $G_i$ $(i = 0, \cdots, v)$ be the ramification groups of $\mathfrak{B}_i$. Then, by the Hilbert formula, $\mathcal{D}$ is exactly divisible by $p^r$ where $r = fg \cdot \sum \{(\#(G_i) - 1) \mid i = 0, \cdots, v\}$. 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 $\xi \in K$ where $\xi$ is a primitive $n$th root of $1$. If $c$ is any $\mathfrak{o}$-ideal class of $K$, there is a cyclic extension $\Delta/K$ of degree $n$ with $C_0(\mathcal{O}(\Delta)) = c^{d(n)}$. (In fact, there are infinitely many such extensions, and they may be chosen so that $\mathcal{D}(\mathcal{O}(\Delta)/\mathfrak{o})$ is relatively prime to any preassigned $\mathfrak{o}$-ideal $\mathfrak{b}$ of $K$.)

The following is an immediate consequence.

**Corollary.** (Same hypothesis.) $\mathcal{D}(\Delta)$ is a free $\mathfrak{o}$-module for every cyclic extension $\Delta/K$ 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 $m$ is any ideal in $\mathfrak{o}$, there are infinitely many prime ideals in any ideal class mod $m$. (The ideal class group mod $m$ is the quotient of the group of all $\mathfrak{o}$-ideals prime to $m$ modulo the subgroup of principal ideals of form $\alpha \cdot \mathfrak{o}$ where $\alpha \equiv 1$ (mod $m$).

First suppose $l$ is odd. Let $c$ be any ideal class and let $t > 1$ be any integer such that $c^t = c$. (We may suppose $t$ is odd.) Let $p$ be any prime ideal in $c$ such that $p \mid l$. Choose distinct primes $p_1, \cdots, p_t$ in the same ideal class mod $m$ as $p$, where we take $m = (1 - \xi)^{t^r}$. Then choose primes $q_1, \cdots, q_t$ in the inverse ideal class of $p$ mod $m$. 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 $1 \leq i \leq (t - 1)/2$, $a_i = l + 1$ for $(t + 1)/2 \leq i \leq t - 1$, and $a_i = l + 2$.) Then $(\prod_{i=1}^t p_i^{a_i}) \cdot (\prod_{i=1}^t q_i^{a_i})^{\ell} = \mu \cdot \mathfrak{o}$, a principal ideal where $\mu \equiv 1$ (mod $m$). If $\alpha$ is a root of $f(x) = X^l - \mu$, then $\Delta = K(\alpha)$ is a cyclic extension of $K$ of degree $l^r$. We show that $C(\mathcal{O}(\Delta)) = c^{(t-1)/2}$. To do this, we must compute $\mathcal{D}(\mathcal{O}(\Delta)/\mathfrak{o})$.

First we show that no higher (i.e., wild) ramification occurs. For let $I$ be a prime of $K$ dividing $l$, and suppose $I^a$ exactly divides $(1 - \xi)$. Let $\mathfrak{q}$ be a prime of $\Delta$ dividing $l$, say $\mathfrak{q}^b$ exactly divides $l$. Now, $1 - \mu = \prod \sigma (1 - \sigma(\alpha))$ where $\sigma$ runs over the Galois group $G$ of $\Delta/K$. Since $1 - \mu$ is divisible by $m = (1 - \xi)^{t^r}$, at least one of the factors (which we may take to be $(1 - \alpha)$) is divisible at least by $\mathfrak{q}^{ab^r}$. But, for any $\sigma \in G$, $\sigma \neq 1$, we have $\sigma(\alpha) - \alpha = (\xi - 1)\alpha$ for some $0 < j < l^r$. Since $\mathfrak{q} \mid \alpha$ and $(\xi - 1) \mid (\xi^{t^r - 1} - 1)$ which is exactly divisible by $\mathfrak{q}^{ab^r - 1}$, we have $\sigma(\alpha) - \alpha$ divisible at most by $\mathfrak{q}^{ab^r - 1}$. Hence, in the $\mathfrak{q}$-adic
metric on $\Delta$, $\alpha$ 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 $\Delta^*$ denote the completions of $K$ and $\Delta$ at $\wp$, we have $\Delta^* = K^*(\alpha) \subseteq K^*(1) = K^*$. Hence, $\wp$ is unramified over $K$ and, indeed, of degree 1 over $K$.

Since $f'(\alpha) = l'(\alpha)^{f-1}$, the only possible divisors of $\wp$ are the divisors of $\mu$. Clearly $p_1, \ldots, p_t$ are completely ramified in $\Delta$ so that $\wp$ is exactly divisible by $p_i^{f-1}$. On the other hand, it is easily seen that the inertial field for any prime divisor of $q_j$ ($1 \leq j \leq t$) is $K((\mu)^{1/2}) = K(\alpha^{f-1})$. (To see this: $q_j$ is unramified in $K((\mu)^{1/2})$, for we can easily find $\mu' = \beta'\mu$ where $q_j$ is prime to $\mu'$ and $K((\mu)^{1/2}) = K((\mu')^{1/2})$. Also, clearly, the ramification index of any divisor of $q_j$ in $\Delta$ is at least $l^{r-1}$, whence it is exactly $l^{r-1}$.) Thus, $\wp$ is exactly divisible by $q_j^{f(r-1)} = q_j^{f-1}$. Hence,

$$\wp^{1/2} = \left( \prod_{i=1}^{t} p_i \right)^{(l^{r-1})/2} \left( \prod_{j=1}^{t} q_j \right)^{(l^{r-1})/2} = p^{t(l^{r-1})/2} \sim p^{t-1}/2.$$ 

(Here, $\sim$ means "belongs to the same ideal class as.") Hence $C(\wp(\Delta)) = c(1-1/2)$. The case $t = 2$ is similar. Choose a prime $p \mid 2$ in the class $c$. Take primes $p_1$ and $p_2$ in the same class mod $m$ as $p$, and take $p_2$ in the class of $p^{2+}$ mod $m$, where $m$ is a power of 2 large enough to avoid higher ramification. Then $p_1 p_2 p_3 = (\mu)$ where $\mu \equiv 1$ (mod $m$). Let $\alpha$ be a root of $f(x) = x^{p^{2+}} - \mu$ and consider $\Delta = K(\alpha)$. Then $\wp = (p_1 p_2)_{2^{2+}-1} p_2^{2+}$. Also, $f'(\alpha) = 2^{2+} \alpha^{2+}-1$, so if $\Delta$ is the discriminant of the basis 1, $\alpha, \alpha^2, \ldots, \alpha^{2+}$, then $(\Delta) = 2^{2+} (\mu)^{2+}-1$. Hence $((\wp/\Delta)^{1/2}) \sim p_3 (2^{2+}-1) p_2^{2+} \sim (p^{t-2}) p_2^{2+} = p$. Hence $C(\wp(\Delta)) = c$. 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 $\Delta_1$ and $\Delta_2$ be linearly disjoint over $K$ (i.e. $\Delta_1 \cdot \Delta_2 = \Delta_1 \otimes_K \Delta_2$). Let $\wp_i = \wp(\Delta_i)$. If $\wp(\Delta_1/o)$ and $\wp(\Delta_2/o)$ are relatively prime, then the maximal $\wp$-order of $\Delta_1 \otimes_K \Delta_2$ is $\wp_1 \otimes \wp_2$ and its discriminant over $\wp$ is $\wp(\Delta_1/o) \otimes [\Delta_1 : K] \wp(\Delta_2/o) \otimes [\Delta_2 : K]$.

**Proof.** Let $\wp'$ be the maximal $\wp$-order of $\Delta_1 \otimes_K \Delta_2$. Then $\wp' \supseteq \wp_1 \otimes \wp_2$, and $\wp(\wp_1 \otimes \wp_2/\wp) = \wp(\wp'/\wp) [\wp': \wp_1 \otimes \wp_2]^2$ where the notation $[M:N]$ denotes the module index (see Fröhlich [2], [3] and [4]). Also,

$$\wp(\wp'/\wp) = N_{\Delta_1/K}(\wp(\wp'/\wp_1)) \cdot \wp(\wp_1/o)^{[\Delta_1 : K]}$$

License or copyright restrictions may apply to redistribution; see http://www.ams.org/journal-terms-of-use
where the pair \((i, j)\) is \((1, 2)\) or \((2, 1)\).

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

We next prove Theorem 2 in the general case. Let \(n = \prod_{i=1}^{s} l_i^{e_i}\) where the \(l_i\) are distinct primes. Let \(d = d(n)\). For each \(i\), let \(d(l_i) = d \cdot h_i\). Then \(\gcd\{h_i | 1 \leq i \leq s\} = 1\) and \((h_i, l_i) = 1\). Hence \(\gcd\{h_i n/l_i^{e_i} | 1 \leq i \leq s\} = 1\). For, suppose to the contrary that the prime \(p\) is a common divisor. We may suppose \(p \mid h_i\) whence \(p \mid (n/l_i^{e_i})\) so \(p = l_2\), say. But then \(p \mid (h_2 n/l_2^{e_2})\).

Choose integers \(x_i\) such that \(\sum \{x_i h_i n/l_i^{e_i} | 1 \leq i \leq s\} = 1\). Then \(d = \sum \{x_i d(l_i) n/l_i^{e_i} | 1 \leq i \leq s\}\). Choose cyclic extensions \(\Lambda_i/K\) of degree \(l_i^{e_i}\) having \(C(\mathfrak{D}(\Lambda_i)) = c^{e_i d(l_i)}\) and such that the \(\mathfrak{D}(\mathfrak{D}(\Lambda_i)/\mathfrak{D})\) 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 \(\mathfrak{D}(\Lambda) \cong \mathfrak{D}(\Lambda_1) \otimes \cdots \otimes \mathfrak{D}(\Lambda_s)\). Hence (see Fröhlich [3, p. 32])

\[
C(\mathfrak{D}(\Lambda)) = \prod \{C(\mathfrak{D}(\Lambda_i))^{n/l_i^{e_i}} | 1 \leq i \leq s\} = c^d.
\]

References

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

University of Illinois