ABSTRACT. Let $k$ be an algebraic number field and $l$ an odd prime. The set of Steinitz classes of tamely ramified cyclic extensions $K/k$ of degree $l^r$ is calculated and shown to be a subgroup of the ideal class group of $k$.

Introduction. In this paper $k$ will denote a (finite) algebraic number field with ring of algebraic integers $O_k$. For a finite extension $K/k$ the ring $O_K$ of integers in $K$ is a module over $O_k$. Such modules are classified up to isomorphism by two invariants: the rank and the Steinitz class. Since the ring $O_K$ is uniquely determined within $K$ it is reasonable to denote the Steinitz class of $O_K$ as an $O_k$-module by $C(K, k)$.

Denote by $G$ a cyclic group of odd prime power order $l^r$. As $K$ varies over the normal extensions of $k$ with Galois group isomorphic to $G$ the associated Steinitz class $C(K, k)$ varies over a subset of the ideal class group $C(k)$ of $k$; this subset is denoted $R(k, G)$. It is the set of ideal classes of $k$ which can be realized as the Steinitz class of the ring of integers in a normal extension $K/k$ with Galois group $G$. The subset $R_l(k, G)$ of $R(k, G)$ consisting of those classes which correspond to tamely ramified extensions is a subgroup of $C(k)$ which will be explicitly described. The reader may find [4] and [6] to be useful introductory references. In reference [4] the problem was studied for the special case $r = 1$. The methods of this paper are the same in broad outline. In order to carry them through it is necessary to be able to construct tamely ramified cyclic extensions $K/k$ of degree $l^r$.

The paper is divided into three parts. In the first it is shown that $R_l(k, G)$ is contained in a certain subgroup of $C(k)$. In the second is given the procedure for constructing tamely ramified cyclic extensions of degree $l^r$, which is then applied in the third to prove that the inclusion shown in part one is in fact an equality.
The entire investigation is founded on a formula for \( C(K, k) \) due to Artin [1]. Following [4], [6] this will be used in the form: \( C(K, k) \) is the class of the square root of the relative discriminant ideal when \( K/k \) is a normal extension of odd degree.

1. The following standard lemma will be useful:

**Lemma.** Let \( K/k \) be an abelian extension of number fields which is tamely ramified at the prime \( \mathfrak{p} \) of \( k \). Then \( N(\mathfrak{p}) \equiv 1 \mod e(\mathfrak{p}, K/k) \). (\( N \) denotes the absolute norm; \( e \) the degree of ramification in the indicated extension.)

**Proof.** Let \( D \) denote the decomposition group of \( \mathfrak{p} \) for \( K/k \) and \( K/\mathfrak{P} \) the residue field of \( K \) at some prime \( \mathfrak{P} \) which divides \( \mathfrak{p} \). Define \( f: D \to (K/\mathfrak{P})^* \) by \( f(\sigma) = \sigma(\mathfrak{p}/\mathfrak{p} \mod \mathfrak{P}) \) where \( \mathfrak{p} \in \mathfrak{P}/\mathfrak{P}^2 \) is a prime element for \( \mathfrak{P} \). The function \( f \) satisfies the identity \( f(\sigma r) = f(\sigma)f(r)^{\sigma} \); the exponent \( \sigma \) on the right means the automorphism of \( K/\mathfrak{P} \) over \( k/\mathfrak{p} \) induced from \( \sigma \). Let \( T \) denote the inertia group of \( \mathfrak{p} \) in \( K/k \); \( r \in T \) iff \( r \) acts trivially on \( K/\mathfrak{P} \).

Since \( D \) is abelian one sees that \( f(\tau) = f(\tau) \forall \tau \in T \). As every automorphism of \( K/\mathfrak{P} \) over \( k/\mathfrak{p} \) is induced by some element of \( D \) it follows that \( f(T) \subseteq (k/\mathfrak{p})^* \). The restriction of \( f \) to \( T \) is a homomorphism so that \( |T||N(\mathfrak{p}) - 1| \); since \( e = |T| \), this completes the proof.

One could also observe that the lemma follows from local class field theory. An extension \( K/k \) will be called "of type \( G \)" if it is normal and its Galois group is isomorphic to \( G \).

**Proposition.** Let \( K/k \) be a tamely ramified extension of type \( G \) and let \( W \) be the subgroup of \( C(k) \) generated by \( \{C(\mathfrak{p}) : \mathfrak{p} \text{ prime}, N(\mathfrak{p}) \equiv 1 \mod l' \} \). Then \( C(K, k) \in W(l'-1)/2 \).

**Proof.** Let \( b \) be the relative discriminant ideal so that \( C(K, k) = C(\sqrt{b}) \) by Artin's theorem. If a prime \( \mathfrak{p} \) of \( k \) splits into \( g \) primes in \( K \) each of degree \( f \) and ramification degree \( e \), then the contribution of \( \mathfrak{p} \) to \( b \) is \( b_{\mathfrak{p}} = \mathfrak{p}^{gf(e-1)} \). Suppose \( e = l', t > 0 \); then \( f = l'^{-t} \). The lemma implies that \( N(\mathfrak{p}) \equiv 1 \mod l'^{t} \); hence \( N(\sqrt{b^{l'^{-t}}}) \equiv 1 \mod l' \). From this it is easy to conclude that \( C(\sqrt{b^{l'^{-t}}}) \in W \). In fact \( W = \{C(\mathfrak{a}) : N(\mathfrak{a}) \equiv 1 \mod l' \} \); for let \( W_0 \) be the indicated set. Then it is obvious from the definition of \( W \) that \( W \subseteq W_0 \). Conversely, suppose \( N(\mathfrak{a}) \equiv 1 \mod l' \). By the generalized "theorem on primes in an arithmetic progression" there is a prime ideal \( \mathfrak{q} \) such that \( a \mathfrak{q}^{-1} \) is a principal ideal with a generator \( a \equiv 1 \mod l' \) (congruence in the ring \( O_k \)). It follows that...
$C(a) = C(q)$ and that $N(q) \equiv 1 \mod l'$, so that $C(a) \in W$.

The proposition should now be clear since for every prime $| \mathfrak{p} | \mathfrak{b}$ we have seen that $C(\mathfrak{b} \mathfrak{p}) \in W^{l-1}$. It follows from the proposition that $R(k, G) \subseteq W^{(l-1)/2}$.

2. In order to prove that $R(k, G)$ and $W^{(l-1)/2}$ are actually equal it is necessary to be able to construct extensions $K/k$ of type $G$. This will be done by constructing Kummer extensions of the field $F = k(\zeta)$ where $\zeta$ is a primitive $l'$th root of unity. In the case $r = 1$ which was studied in [4] an extension $L/F$ of degree $l$ which is abelian over $k$ contains a unique subfield $K$ which is cyclic over $k$; when $r > 1$ the situation is less simple but there proves to be a degree of uniqueness in any case. The construction which will be given does not produce all possible extensions $K/k$ of type $G$ but does give enough for present needs.

In addition to the notation which has already been introduced is the following:

- $\zeta$: primitive $l'$th root of unity,
- $F = k(\zeta)$,
- $Z = \text{cyclic group generated by } \zeta$,
- $m = [F: k]$,
- $H = \text{Gal}(F/k)$,
- $\sigma$: a fixed generator of $H$,
- $s$: defined by $\sigma(\zeta) = \zeta^s$,
- $R = Z/l''Z$,
- $k' = k\setminus\{0\}$ as a group under multiplication.

For $a \in F'$ let $a_i = \sigma^i(a)$ and $a_i$ be an $l'$th root of $a_i$ in some algebraic closure of $k$. Let $N(a) = F(\alpha_0, \ldots, \alpha_{m-1})$. The field $N(a)$ is unambiguously determined by $a$ even though the $\alpha_i$'s are defined only up to a factor $\zeta^i$. When only one $a$ is under consideration $N(a)$ will be written $N$. Let $\mathfrak{G} = \text{Gal}(N/k)$, $X = \text{Gal}(N/F)$, and $E = \{\beta \in N': \beta | l' \in F\}$. There is a nondegenerate bilinear function $\langle , \rangle : E/F' \times X \to Z = \text{the cyclic group generated by } \zeta$ in $F'$ defined by $\langle e, \tau \rangle = \tau(e)/e$.

Let $\sigma_1$ be a fixed element of $\mathfrak{G}$ whose restriction to $F$ is the fixed $\sigma \in H$. $E/F'$ is a left module over the group ring $RH$ by the action $\sigma(eF') = \sigma_1(e)F'$ which will be written $\sigma(e)F'$ from now on. $X$ is a right $RH$-module.
by the action \( x^\sigma = \sigma^{-1} x \sigma \); \( Z \) is a left \( RH \)-module for the Galois action of \( H \) on \( F \). With these actions the isomorphism of abelian groups \( \phi: E/F' \to \text{Hom}(X, Z) \) given by \( \phi(e^F) = \langle e, \cdot \rangle \) is an \( RH \)-isomorphism. \( H \) acts on \( \text{Hom}(X, Z) \) via the left action on \( Z \) and the right action on \( X \) so that \( (\sigma f)(x) = \sigma(f(x^\sigma)) \). This means that

\[
\langle \sigma(e), x \rangle = \sigma(\langle e, x^\sigma \rangle) = \langle e, x^\sigma \rangle^s
\]

so that \( \langle e, x^\sigma \rangle = \langle \sigma(e), x \rangle^{s^{-1}} = \langle s^{-1} e, x \rangle \) where \( s^{-1} \) is to be understood as (a unit) in \( R \). Observe that \( E/F' \) and \( X \) are both cyclic \( RH \)-modules. (For example \( E/F' \) is generated over \( RH \) by \( \alpha_0 F' \).)

The first task is to identify the maximal abelian extension of \( k \) in \( N \).

The following result is easy to prove and probably well known.

**Lemma.** Let \( 0 \to X \to \mathbb{G} \to H \to 1 \) be an extension of an abelian group \( X \) by a cyclic group \( H = \langle \sigma \rangle \). Then the commutator subgroup of \( \mathbb{G} \) is \( i(X^{1-\sigma}) \).

From now on let \( \alpha = \alpha_0^F \) which will be identified with \( \alpha_0 F' \) as an element of \( E/F' \). Any cyclic extension of \( F \) in \( N \) has the form \( F((\Sigma r_i \sigma^i) \alpha) \) for some element \( \Sigma r_i \sigma^i \in RH \). In view of the lemma such an extension is abelian over \( k \) iff

\[
\left\langle \left( \sum r_i \sigma^i \right) \alpha, x^{1-\sigma} \right\rangle = 1 \quad \forall x \in X.
\]

Since \( \langle (\Sigma r_i \sigma^i) \alpha, x^{1-\sigma} \rangle = \langle (\Sigma r_i \sigma^i - \Sigma s^{-1} r_i \sigma^{i+1}) \alpha, x \rangle \), this will be the case iff the element \( \Sigma (r_i - s^{-1} r_{i-1}) \sigma^i \) in \( RH \) annihilates \( \alpha \) in \( E/F' \). (We agree that \( r_{-1} = r_{m+1} \).) As this is certainly the case if each \( r_i = rs^{-i} \) for some \( r \in R \), the following is true.

**Proposition.** Let \( e = \Sigma s^{-i} \sigma^i \in RH \). Then for any \( \beta \in E \), \( F(e\beta) \) is an abelian extension of \( k \).

**Remark.** In the case \( r = 1 \) every cyclic extension \( L/F \) of degree \( l \) which is abelian over \( k \) can be obtained by adjoining \((ea)^{1/l}\) for some \( a \in F' \). The proof of this fact uses the semisimplicity of the group ring \( RH \) and the fact that \( \epsilon \) is a primitive idempotent in \( RH \). In the case being considered here \( RH \) is not semisimple and \( \epsilon \) is not an idempotent; one would expect that in this case there are extensions \( L/F \) of type \( G \) which are abelian over \( k \) but which are not of the form \( L = F((ea)^{1/l'}) \) for any \( a \in F' \). Here is an example of such an extension: Let \( k = Q, l' = 9, F = Q(\zeta) \) where \( \zeta \) is a primitive 9th root of unity. \( L \) will be the field \( F(\zeta^{1/9}) \) which is certainly
abelian over $Q$. In terms of the action of $RH$ on $F'/F''$ it must be shown that $\zeta \neq \epsilon a$ in $F'/F''$ for any $a$. (1) $O_F = \mathbb{Z}[\zeta]$ is a PID, for the relative class number is 1 (cf. Hasse [3]) and the class number of the maximal real subfield $F^+$ is also 1 (cf. tables in [2] or the review problem set III in Samuel [7]). (2) It is now easy to see that if $\zeta = \epsilon a$ then $a$ may be taken as a unit in $F$. (3) Every unit in $F$ has the form $\pm \zeta^i \eta$ where $\eta$ is a unit in $F^+$. (This follows from Satz 23 or 24 in [3].) (4) As 2 is a primitive root mod 9 we may take $\sigma(\zeta) = \zeta^2$. Then for any $\eta \in F^+$, $\epsilon \eta = \Pi \sigma^i(\eta)^{s^{-1}}$, $s^{-1} = 5$ mod 9, $\epsilon(\eta) \in (F^+)^9$. (Note. In general if $a$ lies in a proper subfield of $F$, then $\epsilon a$ is at least an $l$th power in $F$ but not necessarily an $l$th power.) It follows that $\zeta = \epsilon a$ with $a \in F'$, $\zeta = \pm \epsilon \zeta^i$ for some $i$; this is impossible since $\epsilon \zeta \in F^3$, and the example is complete.

Return to the situation described above; $E/F' = RH$. Let $\Sigma = \Sigma_i \sigma^i \in RH$ and let $X_0$ be the kernel of $\Sigma$ acting on $X$. For any $x \in X$, $(\epsilon a, x) = (a, x^2)$ so that $x \in \text{Gal}(N/F(\epsilon a))$ iff $(a, x^2) = 1$. Since $x^2$ is invariant under $H$, $a$ generates $E/F''$ as an RH-module, and the pairing $(,)$ is non-degenerate, it follows that $\text{Gal}(N/F(\epsilon a)) = X_0$. The preceding proposition expresses the fact that $X^{1-\sigma} \subseteq X_0$. Let $L = F(\epsilon a)$; it remains to decide under what circumstances $L$ contains a subfield $K$ which is cyclic of degree $l'$ over $k$. Of course $\text{Gal}(L/k)$ is an extension of $H$ by a cyclic group of order a divisor of $l'$.

**Proposition.** If $a_0, \ldots, a_{m-1}$ are independent over $R$, then $\text{Gal}(L/k) \cong G \times H$.

**Proof.** In this case $E/F'$ is the free RH-module with basis $\{a\}$ and one deduces easily that $X \cong RH$ as well. (In fact $X$ is generated as an RH-module by the automorphism which sends $a$ to $\zeta a$, the action of this automorphism on other elements of $E$ being determined by the action of $H$ on $x$ and $E/F'$.) It follows that $\mathbb{G} \cong X \cdot H$, $X_0 = X^{1-\sigma}$, and $X/X_0 \cong G$, from which the assertion follows.

The hypothesis in the last result can be stated in terms of the $a_i$'s; namely that $a_0, \ldots, a_{n-1}$ should be multiplicatively independent modulo $l'$th powers in $F'$.

If this hypothesis is not satisfied it may happen that a field $L = F(\epsilon a)$ is itself cyclic as an extension of $k$. For example, if $F = Q(\zeta)$, where $\zeta$ is a primitive $l'$th root of unity and $L = F((\epsilon \zeta)^{1/l'})$, this is the case.

From the last proposition one sees that the field $L$ will contain subfields which are cyclic of degree $l'$ over $k$; the final task is to show that
when \( N/F \) is tamely ramified at least one of these extensions is tamely ramified over \( k \).

**Proposition.** Assume \( \alpha_0, \ldots, \alpha_{n-1} \) are independent over \( R \) and assume \( N/F \) is tamely ramified. Let \( K \) be the subfield of \( N \) fixed by \( X_0 \cdot H \), then \( K/k \) is a tamely ramified extension of type \( G \).

**Remark.** The reader may wonder why the field \( L \) was ever mentioned since \( K \) is presented as a subfield of \( N \). Of course \( K \subseteq L \) and it will be useful in the next paragraph to dispense with \( N \).

**Proof.** Suppose \( V = \langle \sigma^h \rangle \) is the (first) ramification group of some prime \( l \) dividing \( (l) \) for the extension \( F/k \). The ramification group in \( N/k \) of any prime \( \mathfrak{p} \) will be generated by an element of the form \( x \cdot \sigma^h \) whose order, say \( l^n \), is the same as that of \( \sigma^h \). In terms of the right action of \( H \) on \( X \) described above the multiplication in \( X \cdot H \) is given by \( (x_1 \cdot \sigma^i)(x_2 \cdot \sigma^j) = x_1 x_2 \sigma^{-i} \cdot \sigma^{i+j} \). Hence \( 1 + \sigma^{-h} + \sigma^{-2h} + \cdots + \sigma^{-(l^n-1)h} \) annihilates \( x \). Since \( X \) is free as a \( V \)-module it follows that \( x \in X^{1-\sigma^h} \subseteq X^{1-\sigma} = X_0 \), and the proposition is proven.

3. The results of §2 make it possible to prove the following

**Theorem.** \( \mathcal{R}(k, G) = \mathbb{W}^{(l-1)/2} \). Given \( A \in \mathbb{W} \) and any ideal \( \mathfrak{b} \) in \( \mathcal{O}_k \), there is a tamely ramified extension \( K/k \) of type \( G \) for which \( C(K, k) = A \) and \( (b_{K/k}, \mathfrak{b}) = 1 \).

**Proof** (compare Theorem (2.6) in [4]). Let \( t > 3 \) be an odd integer such that \( A^t = A \) and choose positive integers \( h_1, \ldots, h_t \) relatively prime to \( l \) so that \( \sum h_i = lt \). Choose primes \( \mathfrak{p}_1, \ldots, \mathfrak{p}_t \) relatively prime to \( \mathfrak{b} \) in \( F \) each of which splits completely in \( F/k \), no two of which are conjugate in \( F/k \), and so that each \( \mathfrak{p}_i \cap k \) is in the class \( A \). Assume also that all the \( \mathfrak{p}_i \)'s are in the same ideal class modulo a sufficiently high power of \( l \) and let \( q_i, i = 1, \ldots, t \), be nonconjugate prime ideals in the inverse class. Then the ideal

\[
\mathfrak{p}_1^h \cdots \mathfrak{p}_t^h (q_1 \cdots q_t)^l
\]

is a principal ideal generated by some \( a' \in F \) which is congruent to \( 1 \) modulo a high power of \( l \). To insure that the conjugates of \( a' \) will be multiplicatively independent modulo \( l^r \)th powers in \( F \) let \( a = \rho a' \), where \( (\rho) \) is a prime ideal not dividing \( \mathfrak{b} \) which splits completely in \( F/k \), and \( \rho \equiv 1 \) modulo a high power of \( l \). The conditions satisfied by \( a \) insure that the con-
jugates \( \sigma^i(a) \) are independent over \( R \) (acting exponentially) and that the field \( N(a) \) described in §2 is tamely ramified over \( F \).

(Indeed, if \( \mathfrak{U} \) is a prime divisor of \((l)\) in \( F \), the condition \( a \equiv 1 \mod \mathfrak{U} \) means any power \( n \) so high that, for each \( \mathfrak{U} | (l) \) in \( F \), \( a \equiv 1 \mod \mathfrak{U}^n \) implies \( a \) is an \( l \)-th power in \( F \).) Now let \( K \) be the subfield of \( N(a) \) described in §2. Then \( L = KF \) and \( \mathfrak{b}_{L/F} = \mathfrak{b}_{K/k} \) as ideals in \( \mathcal{O}_F \). Let \( P_i = \prod_j \sigma^i(\mathfrak{b}_i) \), \( Q_i = \prod_j \sigma^j(\mathfrak{q}_i) \); these are prime ideals in \( \mathcal{O}_k \). It is easy to see that

\[
\mathfrak{b}_{L/F} = \prod_i P_i^{r-1} Q_i^{l(r-1) - 1} \cdot (\rho)^n
\]

for some \( n \). From this it follows that \( C(K, k) = A^{(l-1)/2} \).

4. In general \( R(k, G) \) will be a union of cosets of \( R_k(k, G) \) within the ideal class group \( C(k) \). For a given field \( k \) it can be described explicitly in terms of the structure of the groups of principal units in the completions \( k_i \) of \( k \) at primes \( \mathcal{U} | (l) \). More specifically suppose that \( \mathcal{U}_1, \ldots, \mathcal{U}_g \) are the primes of \( k \) which divide \((l)\). Suppose that for each \( i \) there is given an ideal \( \mathcal{U}_i^{e_i} \) which is the discriminant of some extension of type \( G \) of the local field \( k_i \) = completion of \( k \) at \( \mathcal{U}_i \). Then by Grunwald's theorem there is an extension \( K_1/k \) of type \( G \) with discriminant \( \Pi_i \mathcal{U}_i^{e_i} \cdot \mathfrak{b} \) where \( (\mathfrak{b}, (l)) = 1 \). (This depends on the fact that \( l > 2 \).) From the proof of the proposition in §1 it follows that \( C(\mathfrak{b}) \in \mathcal{W}^{(l-1)/2} \). Now suppose \( A \in \mathcal{W} \). By the theorem there is a tamely ramified extension \( K_2/k \) of type \( G \) whose discriminant is relatively prime to \((l)b\) and for which

\[
C(K_2, k) = (A \cdot C(\mathfrak{b}))^{-1/2} \cdot A^{(l-1)/2}.
\]

The composite \( K_1K_2 \) contains a subfield \( K \) which is of type \( G \) over \( k \) and for which \( \mathfrak{b}_K = \mathfrak{b}_1 \mathfrak{b}_2 \cdot (\mathfrak{b}_i \) is the discriminant of \( K_i/k \). One can take for \( K \) the field fixed by the "diagonal subgroup" of \( \text{Gal}(K_1K_2/k) \), cf. Lemma (4.3) in [4].) It follows that

\[
C(K, k) = A^{(l-1)/2} \cdot \prod_i C(\mathcal{U}_i)^{e_i/2}
\]

so that \( R(k, G) \) is determined by which exponents \( e_i \) may occur. An example of a field \( k \) and a group \( G \), elementary abelian of type \((3, 3)\), for which \( R(k, G) \) is not a group is given in [5]. Of course when \( G \) is cyclic of order \( l \), \( R(k, G) \) proves to be a group. I do not yet know exactly what happens in the case \( G \) cyclic of order \( l^r \).
REFERENCES


