PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 142, Number 1, January 2014, Pages 21–28
S 0002-9939(2013)11729-6
Article electronically published on September 10, 2013

CLASS GROUPS IN CYCLIC ℓ-EXTENSIONS: COMMENTS ON A PAPER BY G. CORNELL

MICHAEL ROSEN

(Communicated by Matthew A. Papanikolas)

Abstract. Let E/F be a cyclic extension of number fields of degree ℓ^n, where ℓ is a prime. It is proved that the ℓ-rank of the class group of E is bounded by $\ell^n(t-1+\mathrm{rk}_\ell Cl_F)$, where t is the number of primes of F, including infinite primes, which ramify in E and Cl_F is the class group of F. This generalizes a result of G. Cornell which applies when $n=1$ and ℓ is odd. A similar result is shown to hold when the Galois group is an abelian ℓ-group and the Hasse norm theorem is valid for E/F.

Let E/F be a Galois extension of number fields whose Galois group G is a ℓ-group. In a paper published in 1983, G. Cornell gives an upper bound for the ℓ-rank of the class group of E, Cl_E, in terms of the ℓ-rank of Cl_F, the ramification of primes of F in E, and the degree $[E:F]$ (see Theorem 4 of [2]). The only restriction he places on his results is that ℓ not be equal to 2. In this paper, we remove this restriction and also show that in the special case where G is cyclic, the same method often leads to a stronger result. In fact, we can also prove that a variant of our result holds for abelian ℓ-extensions E/F for which the Hasse norm theorem is true. See Theorems 2.2 and 3.2 which are stated below.

To fix ideas and notation, we start with the formal definition of an ℓ-rank. In this paper, ℓ denotes any prime number. For a finite abelian group A, we define the ℓ-rank of A to be the dimension over $\mathbb{Z}/\ell\mathbb{Z}$ of $A/\ell A$. We denote the ℓ-rank of A by $\mathrm{rk}_\ell(A)$.

Section 1. Preliminaries

Recall that the genus field of E with respect to F, $\tilde{E}_F$ is the maximal abelian unramified extension of E which is of the form KE, where K is an abelian extension of F. Let H_E be the Hilbert class field of E. Set $C=\mathrm{Gal}(H_E/E)$ and $\mathcal{G}=\mathrm{Gal}(H_E/F)$. Since C is abelian, the exact sequence $1\to C\to\mathcal{G}\to G\to 1$ leads to an action of G on C. Using class field theory we can identify the action of G on C with the action of G on $Cl_E\cong C$.

When G is abelian it is clear that $\tilde{E}_F$ is an abelian extension of F and that the corresponding subgroup of $\mathcal{G}$ is $[\mathcal{G},\mathcal{G}]$. The Galois group of $\tilde{E}_F$ over E is isomorphic to $C/[\mathcal{G},\mathcal{G}]$. The following is a restatement of Proposition 3 in [2].

Received by the editors March 9, 2011 and, in revised form, December 21, 2011 and February 23, 2012.

2010 *Mathematics Subject Classification.* Primary 11R29.

Key words and phrases. ℓ-rank, class groups, genus field, central class field.

Proposition 1.1. *Assume G is cyclic generated by γ. Let $\mathbb{Z}[G]$ be the group ring of G over $\mathbb{Z}$ and let $I_G = \mathbb{Z}[G](1-\gamma)$ be the kernel of the augmentation map $\sum_\sigma a(\sigma)\sigma \to \sum_\sigma a(\sigma)$. Then,*

$$\mathrm{Gal}(\tilde{E}_F/E) \cong Cl_E/I_G Cl_E \ .$$

It is worth noting that $I_G Cl_E$ is the subgroup of Cl_E consisting of all elements a^γ/a as a runs through Cl_E.

If A is any finite abelian group, we define $A(\ell)$ to be the ℓ-primary subgroup of A. We are interested in the ℓ-rank of Cl_E. This is the same as the ℓ-rank of $Cl_E(\ell)$. Let's define the ℓ-subfield of the genus field of E/F to be the maximal unramified abelian ℓ-extension of E of the form KE, where K is an abelian ℓ-extension of F. Denote this field by $\tilde{E}_F^{(\ell)}$. By working with the ℓ-part of the Hilbert class field of E, the proof of Proposition 1.1 can be adapted to prove the following result.

Proposition 1.2. *Assume G is cyclic of ℓ-power order. Then,*

$$\mathrm{Gal}(\tilde{E}_F^{(\ell)}/E) \cong Cl_E(\ell)/I_G Cl_E(\ell) \ .$$

We want to find a bound for $\mathrm{rk}_\ell Cl_E(\ell)$ in terms of the ℓ-rank of $Cl_E(\ell)/I_G Cl_E(\ell)$. We will initially only assume that G is an abelian ℓ-group, although the main application will be to the case when G is cyclic.

Let A be a finite abelian ℓ-group acted on by a finite abelian ℓ-group G. Let ℓ^m be the exponent of A, and ℓ^n be the order of G. Then, we can consider A to be a module for the group ring $R = (\mathbb{Z}/\ell^m\mathbb{Z})[G]$. Let I_G be the kernel of the augmentation map from R to $\mathbb{Z}/\ell^m\mathbb{Z}$. This is an inessential change in the definition of I_G from that given above. The ideal I_G is the set of all elements of the form $\sum_\sigma a(\sigma)(\sigma-1)$, where $a(\sigma) \in \mathbb{Z}/\ell^m\mathbb{Z}$. Let M be the ideal $\ell R + I_G$.

Lemma 1.3. *M is a maximal ideal which is nilpotent. Consequently, R is a local ring with M being its only maximal ideal. Also, $R/M \cong \mathbb{Z}/\ell\mathbb{Z}$.*

Proof. We first show that I_G is nilpotent. Let $\alpha = \sum_\sigma a(\sigma)(\sigma-1) \in I_G$. Raising both sides to the ℓ-th power we find $\alpha^\ell \in \sum_\sigma R(\sigma^\ell - 1) + \ell R$. By induction we find $\alpha^{\ell^k} \in \sum_\sigma R(\sigma^{\ell^k} - 1) + \ell R$. Recall that ℓ^n is the order of G. Then, it follows that $\alpha^{\ell^n} \in \ell R$. From this we see that $\alpha^{m\ell^n} \in \ell^m R = (0)$. Thus, every element in I_G is nilpotent. Since R is commutative and I_G is finitely generated, it follows that I_G is nilpotent. Since ℓR is clearly nilpotent, M is the sum of two nilpotent ideals and is thus nilpotent itself.

Now,

$$(0) \to M/I_G \to R/I_G \to R/M \to (0)$$

is exact. We know that $R/I_G \cong \mathbb{Z}/\ell^m\mathbb{Z}$. Also, $M/I_G = \ell R + I_G/I_G = \ell(R/I_G) \cong \ell(\mathbb{Z}/\ell^m\mathbb{Z})$. It follows that $R/M \cong \mathbb{Z}/\ell\mathbb{Z}$. Thus, M is a maximal ideal. Since it is nilpotent, R must be a local ring. The proof is complete. □

We need one more lemma which involves the norm element of R. By definition, the norm element is $N = \sum_{\sigma \in G} \sigma$. Clearly, $RN = (\mathbb{Z}/\ell^m\mathbb{Z})N \cong \mathbb{Z}/\ell^m\mathbb{Z}$.

Lemma 1.4. *The ℓ-ranks of R and R/NR are given by*

$$\text{(a)} \quad \mathrm{rk}_\ell(R) = \ell^n$$

and

$$\text{(b)} \quad \mathrm{rk}_\ell(R/NR) = \ell^n - 1.$$

Proof. The first part is obvious since R is the direct sum of $\ell^n = \#(G)$ cyclic groups of order ℓ^m. The second part is also "obvious", but our proof is a little indirect.

We prove a more general fact which implies part (b) as a special case. Let

$$(0) \to A \to B \to C \to (0)$$

be an exact sequence of finitely generated $\mathbb{Z}/\ell^m\mathbb{Z}$-modules. Suppose A and B are free. Then C is also free and the sequence splits. To see this pass to the Pontryagin duals. We find $(0) \to \hat{C} \to \hat{B} \to \hat{A} \to (0)$. The Pontryagin dual of a finite abelian group D is isomorphic to D. In particular, $\hat{A} \cong A$, which is free. Thus the sequence of duals must split. We have $\hat{B} \cong \hat{A} \oplus \hat{C}$. Now, we dualize again and we find $B \cong A \oplus C$. Using the structure theorem for finite abelian groups we see that C is free, which proves our "general fact". Now apply this to the case where $A = RN$ and $B = R$ and use part (a). The lemma follows. □

Proposition 1.5. *The ℓ-rank of A is bounded as follows:*

$$\text{(a)} \quad \mathrm{rk}(A) \le \ell^n \mathrm{rk}(A/I_G A).$$

Moreover, if N annihilates A we have

$$\text{(b)} \quad \mathrm{rk}(A) \le (\ell^n - 1)\mathrm{rk}(A/I_G A).$$

Proof. To ease notation, let's set $A' = A/I_G A$. By Lemma 1.3, R is a Noetherian local ring with M as its maximal ideal. Thus, the minimal number of generators of A as an R-module is the dimension of A/MA over the residue class field $R/M \cong \mathbb{Z}/\ell\mathbb{Z}$, i.e. $\mathrm{rk}_\ell(A/MA)$.

We claim that $\mathrm{rk}_\ell(A/MA) = \mathrm{rk}_\ell(A')$. To see this, note that

$$A/MA \cong (A/I_G A)/(MA/I_G A) = (A/I_G A)/(\ell A + I_G A) \ / \ I_G A) \ .$$

Now, $(\ell A + I_G A)/I_G A = \ell(A/I_G A)$. Thus, $A/MA \cong A'/\ell A'$, which shows that $\mathrm{rk}_\ell(A/MA) = \mathrm{rk}_\ell(A')$ as asserted.

Let's denote $\mathrm{rk}_\ell(A')$ by d. We have shown that A is the epimorphic image of the direct sum of d copies of R. Since the ℓ-rank of R is ℓ^n, it follows that $\mathrm{rk}(A) \le \ell^n d = \ell^n \mathrm{rk}_\ell(A')$.

If the norm element N annihilates A, then we can replace R with R/NR in the above argument. By Lemma 1.4, the ℓ-rank of R/NR is $\ell^n - 1$. We conclude that $\mathrm{rk}_\ell(A) \le (\ell^n - 1)\mathrm{rk}_\ell(A')$. □

This proposition generalizes Proposition 5 of Cornell's paper [2], where the group G is assumed cyclic of order ℓ.

Section 2. The main theorem

In this section we assume that $G = \mathrm{Gal}(E/F)$ is cyclic of order ℓ^n where ℓ is an arbitrary prime. We will apply Proposition 1.5 to the case $A = Cl_E(\ell)$. The integer m is defined to be the smallest positive integer such that ℓ^m annihilates $Cl_E(\ell)$.

Before stating and proving our main result, we recall the definition of the ramification group of an infinite prime. Let E be an algebraic number field. We will think of a prime on E as an equivalence class of absolute values. The infinite primes on F are defined by embeddings of F into the complex numbers $\mathbb{C}$. If $\lambda : F \to \mathbb{C}$ is such an embedding, the corresponding absolute value is $|a|_\lambda = |\lambda(a)|$, where $|z|$ is the usual absolute value of a complex number. If the image of λ lies in $\mathbb{R}$ we say that λ is a real prime; if the image of λ is not in $\mathbb{R}$ we say λ is a complex prime. If λ is a complex prime it defines the same absolute value on E as its complex conjugate, so a complex embedding and its complex conjugate embedding give rise to the same infinite prime of E. Now suppose E/F is an extension of number fields and λ is an embedding of E and λ_0 is its restriction to F. We say that λ is ramified over λ_0 if λ is complex and λ_0 is real. Otherwise we say that λ is unramified over λ_0. If E/F is Galois with group G and λ is an embedding ramified over λ_0, there is a unique $\sigma \in G$ of order 2 such that for all $a \in E$ we have $\lambda(\sigma a) = \overline{\lambda(a)}$. The group generated by σ is, by definition, the ramification group of λ over λ_0. If λ over λ_0 is unramified, we define the ramification group of λ over λ_0 to be $\langle e \rangle$. The main property of these groups which we will use is contained in the following proposition.

Proposition 2.1. *Let E/F be a Galois extension of algebraic number fields with group G. Let H be a subgroup of G and K its fixed field. If all the ramification groups at infinite primes of E are contained in H, then K/F is unramified at all the infinite primes of F.*

The proof of this proposition is straightforward from the definitions, so we leave it to the reader.

From now on in this paper, a prime of a number field will refer to either a finite or an infinite prime.

We are now in a position to state and prove our main result. It should be emphasized that the basic idea of the proof is due to G. Cornell. His proof covers the case in which G is cyclic of odd prime order.

Theorem 2.2. *Let ℓ be a prime number and E/F be a Galois extension of number fields with $G = \mathrm{Gal}(E/F)$ cyclic of order ℓ^n. Let t be the number of primes (finite or infinite) in F which are ramified in E. If E/F is unramified, $\mathrm{rk}_\ell Cl_E \leq \ell^n \ \mathrm{rk}_\ell Cl_F$. If $t \geq 1$,*

$$\mathrm{rk}_\ell Cl_E \leq \ell^n (t - 1 + \mathrm{rk}_\ell Cl_F) \ .$$

In the case where the class number of F is not divisible by ℓ, we have

$$\mathrm{rk}_\ell Cl_E \leq (\ell^n - 1)(t - 1) \ .$$

Proof. To begin with, assume E/F is unramified. Then, $\tilde{E}_F^{(\ell)}/F$ is unramified, as is any abelian ℓ-extension K/F such that KE/E is unramified. It follows easily that $\tilde{E}_F^{(\ell)} = H_F^{(\ell)} E$, where $H_F^{(\ell)}$ is the ℓ-part of the Hilbert class field of F. From this we see that $\mathrm{Gal}(\tilde{E}_F^{(\ell)}/E)$ is isomorphic to a subgroup of $Cl_F(\ell) \cong \mathrm{Gal}(H_F^{(\ell)}/F)$. From Proposition 1.2 and Proposition 1.5, part (a), we deduce $\mathrm{rk}_\ell Cl_E \leq \ell^n \ \mathrm{rk}_\ell Cl_F$. This concludes the proof of our first assertion.

We recall that when G is abelian, the genus field $\tilde{E}_F^{(\ell)}$ is an abelian extension of F. Let $\mathcal{G} = \mathrm{Gal}(\tilde{E}_F^{(\ell)}/F)$. If $\mathfrak{p}$ is a prime of F, the ramification subgroup of $\mathfrak{p}$ in $\mathcal{G}$, $T_{\mathfrak{p}}$, is isomorphic to the ramification group of $\mathfrak{p}$ in G. This follows from the fact that $\tilde{E}_F$ is unramified over E. Since we are assuming that G is cyclic, it follows that all the ramification subgroups of $\mathcal{G}$ are cyclic.

Now, assume $t \geq 1$ and suppose $\{\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_t\}$ is the complete set of primes of F which ramify in E. Let the corresponding ramification subgroups of $\mathcal{G}$ be denoted by $\{T_1, T_2, \ldots, T_t\}$. Let L be the fixed field of T_1. Then, $\tilde{E}_F^{(\ell)}/L$ is totally ramified at primes of L above $\mathfrak{p}_1$ and L/F is ramified at at most $t-1$ primes of F (since it is unramified at $\mathfrak{p}_1$). We claim that $\tilde{E}_F^{(\ell)} = LE$. This is because $\tilde{E}_F^{(\ell)}$ over LE is simultaneously totally ramified at primes above $\mathfrak{p}_1$ and unramified since it is contained in the unramified extension $\tilde{E}_F^{(\ell)}/E$. It follows that $\mathrm{Gal}(\tilde{E}_F^{(\ell)}/E)$ maps, by restriction, injectively into $\mathrm{Gal}(L/F)$.

Since all the T_i are cyclic, the ramification groups of $\mathfrak{p}_2, \ldots, \mathfrak{p}_t$ in $\mathrm{Gal}(L/F)$ are also cyclic. Let $R \subseteq \mathrm{Gal}(L/F)$ be their product and K be the fixed field of R. Since R is the product of at most $t-1$ cyclic ℓ-groups, we have $\mathrm{rk}_\ell R \leq t-1$. On the other hand, K/F is unramified everywhere, including the primes at infinity. It follows that Cl_F maps onto $\mathrm{Gal}(K/F)$. Putting all of this together, we conclude that

$$\mathrm{rk}_\ell \mathrm{Gal}(\tilde{E}_F/E) \leq \mathrm{rk}_\ell \mathrm{Gal}(L/F) \leq t - 1 + \mathrm{rk}_\ell Cl_F \ .$$

From Proposition 1.2 and Proposition 1.5, part (a), applied to $A = Cl_E(\ell)$ we find that

$$\mathrm{rk}_\ell Cl_E \leq \ell^n \mathrm{rk}_\ell (Cl_E(\ell)/I_G Cl_E(\ell)) = \ell^n \mathrm{rk}_\ell \mathrm{Gal}(\tilde{E}_F^{(\ell)}/E) \leq \ell^n (t - 1 + \mathrm{rk}_\ell Cl_F) \ .$$

This proves the second assertion of the theorem.

Finally, assume the class number of F is not divisible by ℓ. Then, $Cl_F(\ell)$ is trivial. It follows that $\mathrm{rk}_\ell(Cl_F) = 0$ and that the norm element annihilates $Cl_E(\ell)$. Using this information, Proposition 1.2, and applying part (b) of Proposition 1.5, we derive, by the same sequence of steps as above, the inequality $\mathrm{rk}_\ell Cl_E \leq (\ell^n - 1)(t-1)$. □

Section 3. A generalization

In this section, we will add a comment on Theorem 2.2 and sketch a generalization.

To begin with, we compare our Theorem 2.2 with Theorem 4 of Cornell's paper [2]. Suppose $E = F_n \supset F_{n-1} \supset \cdots \supset F_0 = F$ is a chain of number fields with F_{i+1}/F_i cyclic of degree $\ell \neq 2$. Suppose t_i primes of F_i ramify in F_{i+1}. If $t_i \geq 1$ set $e_i = t_i$. Otherwise, set $e_i = 1$. Cornell's Theorem 4 states that

$$\mathrm{rk}_\ell Cl_E \leq \sum_{i=0}^{n-1} \ell^{n-i}(e_i - 1) + \ell^n \mathrm{rk}_\ell Cl_F \ ,$$

and if ℓ does not divide the class number of F, one has

$$\mathrm{rk}_\ell Cl_E \leq \sum_{i=0}^{n-1} \ell^{n-i}(e_i - 1) - \ell^{n-1}(e_0 - 1) \ .$$

In [2] the first sum starts from $i = 1$, but this is a misprint. It should start from $i = 0$.

Both results follow from the case $n = 1$ of Theorem 2.2 and are proved by a straightforward induction. This result is very general but a little difficult to apply because of the need to compute the numbers e_i. In the special case of cyclic extensions, Theorem 2.2 shows that one needs only the one number t. Moreover, in this special case, it usually gives a somewhat stronger conclusion. To see this consider a cyclic extension of $\mathbb{Q}$ of odd degree ℓ^n with exactly $t \geq 1$ primes of $\mathbb{Q}$ ramified in E. We also assume each ramified prime is totally ramified. Using the theory of cyclotomic fields, it is not hard to construct such extensions. It is immediate that $e_i = t_i = t$ for all i. By Cornell's second inequality, we find $\mathrm{rk}_\ell Cl_E \leq (\sum_{i=0}^{n-1} \ell^{n-i} - \ell^{n-1})(t-1)$. On the other hand, Theorem 2.2 yields $\mathrm{rk}_\ell Cl_E \leq (\ell^n - 1)(t-1)$, which is smaller as soon as $n \geq 2$ and is considerably smaller when n is large.

Next, we want to explain why we proved Proposition 1.5 for any abelian ℓ-group G, but in Theorem 2.2 we use it only in the case when G is cyclic. To this end we recall the notion of the central class field and compare it to the genus field (see Y. Furuta [3]).

Let E/F be a Galois extension of number fields with group G. The central class field of E/F is defined to be the maximal unramified extension $\hat{E}_F$ of E which is Galois over F and has the property that $\mathrm{Gal}(\hat{E}_F/E)$ is in the center of $\mathrm{Gal}(\hat{E}_F/F)$. As in Section 1, let H_E be the Hilbert class field of E, $C = \mathrm{Gal}(H_E/E)$, and $\mathcal{G} = \mathrm{Gal}(H_E/F)$. It is easy to see that the subgroup of $\mathcal{G}$ corresponding to $\hat{E}_F$ is $[\mathcal{G}, C]$ and the subgroup corresponding to $\tilde{E}_F$ is $[\mathcal{G}, \mathcal{G}] \cap C$ (we are not assuming yet that G is abelian). It follows that the genus field is contained in the central class field. In general these fields are different, as can be seen by means of the formulas Furuta provides for their degree over E: equation (2) on page 319 of [3] and in the statement of Satz 1 on pages 320-21 of the same article. We note that there is a misprint in formula (2): $[K_0 : K]$ should be $[K_0 : k]$. The following result is an almost immediate consequence of these formulas.

Proposition 3.1. *Suppose E/F is a Galois extension of number fields for which the Hasse Norm Theorem (HNT) holds (i.e. every element of F^* which is a norm everywhere locally is a global norm). Then $\tilde{E}_F = \hat{E}_F$.*

Proof. Comparing the formulas of Furuta referred to above, it is enough to show that $[k^* \cap N_{K/k} J_K : N_{K/k} K^*] = 1$ and that $[E_k : E_k \cap N_{K/k} K^*] = [E_k : E_k \cap N_{K/k} U_K]$. We are using the notation of Furuta's paper where K/k is a Galois extension of number fields. The ideles of K are denoted by J_K, and the unit ideles of K are denoted by U_K. The units of K and k are denoted by E_K and E_k respectively. The first equality is equivalent to the HNT. To see the second equality it is sufficient to show that $E_k \cap N_{K/k} K^* = E_k \cap N_{K/k} U_K$ when the Hasse Norm Theorem holds. To show that the left hand side is contained in the right hand side, use the fact that a unit which is a local norm must be the local norm of a local unit. If $\alpha \in E_k$ is in $N_{K/k} U_K$, it must be in $N_{K/k} K^*$ by the HNT. Thus, the right hand side is a subset of the left hand side. It follows that the two sides are equal. $\square$

Since the Hasse Norm Theorem is true for cyclic extensions, the genus field is equal to the central class field in this case. This also follows from the much more elementary fact that a group which is a central extension by a cyclic group is abelian.

Since the subgroup of $\mathcal{G}$ corresponding to $\hat{E}_F$ is $[\mathcal{G}, C]$, we see that $\mathrm{Gal}(\hat{E}_F/E) \cong C/[\mathcal{G}, C]$ is, via the Artin map, isomorphic to $Cl_E/I_G Cl_E$. So, in general this quotient belongs to the central class field, not the genus field. However, when G is cyclic, both fields coincide. This provides a deeper understanding of Proposition 1.1.

These considerations also enable us to generalize Theorem 2.2 to the case where the HNT is valid for E/F. In fact, it would be enough to generate the hypothesis that the genus class field is equal to the central class field. However, I know of no general way to check this hypothesis except via the HNT.

Before stating the theorem, we note that HNT is valid whenever there is a prime P in E whose decomposition group is equal to the whole Galois group. See pages 198-99 of J. Tate's article in [7]. If this happens at a prime which is unramified over F, this forces the Galois group to be cyclic. So, we get something new only when it happens at a prime P which is ramified over F. For example, HNT holds whenever there is a prime in F which is totally ramified in E. A family of examples is given by the cyclotomic fields $K_n = \mathbb{Q}(\zeta_{2^{n+1}})$ for $n \geq 2$. The Galois group $\mathrm{Gal}(K_n/K)$ is a cyclic group of order 2 times a cyclic group of order 2^{n-1}. Nevertheless, HNT holds, since 2 is totally ramified in all of these extensions.

It might be of interest to give an example where one can use Tate's criterion at a prime which is neither unramified nor totally ramified. Consider the extension $K = \mathbb{Q}(\sqrt{5}), \sqrt{-1})/\mathbb{Q}$. The prime (2) of $\mathbb{Q}$ is inert in $\mathbb{Q}(\sqrt{5})$, and the prime above (2) in $\mathbb{Q}(\sqrt{5})$, P say, is totally ramified in K. Set $P = \mathcal{P}^2$. Then the decomposition group of $\mathcal{P}$ over $\mathbb{Q}$ is the full Galois group $\mathrm{Gal}(K/\mathbb{Q})$, but 2 is not totally ramified in K. Nevertheless, the HNT holds for this extension. It is easy to construct many examples of this type.

Theorem 3.2. *Let ℓ be a prime and suppose E/F is an abelian ℓ-extension of number fields of degree ℓ^n for which the Hasse Norm Theorem holds. Let t be the number of finite primes of F which are tamely ramified plus, when $\ell = 2$, the number of infinite primes of F ramified in E. Let $\epsilon_\ell = 1$ if at least one prime of F above ℓ is ramified in E. Otherwise, set $\epsilon_\ell = 0$. Then,*

$$\mathrm{rk}_\ell Cl_E \leq \ell^n(t + 2\epsilon_\ell[F : \mathbb{Q}] - 1 + \mathrm{rk}_\ell Cl_F) \ .$$

In the case that ℓ does not divide the class number of F, we have

$$\mathrm{rk}_\ell Cl_E \leq (\ell^n - 1)(t + 2\epsilon_\ell[F : \mathbb{Q}] - 1) \ .$$

Proof. Since E/F is an ℓ-extension, finite primes of F which do not lie above ℓ are tamely ramified in E and consequently have cyclic ramification groups. The ramification groups of primes lying above ℓ are wildly ramified in E, and the ramification groups can well be non-cyclic. Nevertheless, local class field theory enables us to bound their ℓ-rank. Let $\{\mathfrak{q}_1, \ldots, \mathfrak{q}_r\}$ be the primes of F which lie above ℓ and are ramified in E. Let F_i be the completions of F at $\mathfrak{q}_i$ and E_i the completion of E at some prime lying above $\mathfrak{q}_i$. The Galois group, G_i, of E_i over F_i is isomorphic to the decomposition group of $\mathfrak{q}_i$ in E. With this identification, it is a fact (see the corollary to Proposition 13 of Chapter XIII in [6]) that the norm residue map sends U_i, the local units in F_i^*, onto the ramification group T_i of $\mathfrak{q}_i$ in E. Thus, $\mathrm{rk}_\ell T_i \leq \mathrm{rk}_\ell(U_i/U_i^\ell) = [F_i : \mathbb{Q}_\ell] + \delta_i$, where $\delta_i = 1$ if F_i contains a primitive ℓ-th root of unity and is 0 otherwise. Thus,

$$\mathrm{rk}_\ell \prod_{i=1}^{r} T_i \leq \sum_{i=1}^{r}([F_i : \mathbb{Q}_\ell] + \delta_i) \leq [F : \mathbb{Q}] + r \leq 2[F : \mathbb{Q}] \ .$$

We have used the fact that the sum of the local degrees is equal to the global degree.

To sum up, we have shown that all the ramification groups of E/F are either cyclic or belong to primes in F lying above ℓ and have explicitly bounded ℓ-ranks. The other main tools in the proof of Theorem 2.2 are Proposition 1.2 and Proposition 1.5. For Proposition 1.2 we assumed G is cyclic, but we have seen above that the conclusion of that proposition holds if E/F satisfies HNT. As for Proposition 1.5, it holds for any abelian ℓ-extension. With these remarks it is now an easy matter to show that the proof of the present theorem will follow almost word for word from the proof of Theorem 2.2. □

Readers who would like to know more about the Hasse Norm Theorem should consult D. Garbanati [4] and M. Razar [5].

Acknowledgments

The author would like to thank Reinier Bröker for raising the question about upper bounds for the ℓ-rank in cyclic ℓ-extensions. The question arose in the course of his joint work with D. Gruenwald and K. Lauter [1]. In their paper they are concerned with extensions which are cyclic of order 4.

Thanks are also due to the referee for comments on an earlier version of this paper, in which the problem at $\ell = 2$ was dealt with by using cohomological methods. The referee pointed out that our results were weaker in a number of respects from those of Cornell when ℓ is not equal to 2. This led to a reconsideration of exactly where in [2] the restriction to odd primes is used. As we showed, with small modification, the methods of Cornell's paper apply also in the case $\ell = 2$.

References

[1] R. Bröker, D. Gruenewald, and K. Lauter, *Explicit CM theory for level 2-structures on abelian surfaces*, Algebra Number Theory **5** (2011), 455–528. MR2870099

[2] Gary Cornell, *Relative genus theory and the class group of l-extensions*, Trans. Amer. Math. Soc. **277** (1983), no. 1, 421–429, DOI 10.2307/1999365. MR690061 (84i:12002)

[3] Yoshiomi Furuta, *Über die Zentrale Klassenzahl eines relativ-galoisschen Zahlkörpers*, J. Number Theory **3** (1971), 318–322 (German, with English summary). MR0297743 (45 #6795)

[4] Dennis A. Garbanati, *The Hasse norm theorem for non-cyclic extensions of the rationals*, Proc. London Math. Soc. (3) **37** (1978), no. 1, 143–164. MR0491599 (58 #10822)

[5] Michael J. Razar, *Central and genus class fields and the Hasse norm theorem*, Compositio Math. **35** (1977), no. 3, 281–298. MR0466073 (57 #5956)

[6] Jean-Pierre Serre, *Local fields*, Graduate Texts in Mathematics, vol. 67, Springer-Verlag, New York, 1979. Translated from the French by Marvin Jay Greenberg. MR554237 (82e:12016)

[7] J. T. Tate, *Global class field theory*, Algebraic Number Theory (Proc. Instructional Conf., Brighton, 1965), Thompson, Washington, D.C., 1967, pp. 162–203. MR0220697 (36 #3749)

Department of Mathematics, Brown University, Providence, Rhode Island 02912
E-mail address: mrosen@math.brown.edu