ACTA ARITHMETICA
160.1 (2013)

# Tate sequences and lower bounds for ranks of class groups

by

Cornelius Greither (München)

**1. Introduction.** Consider a Galois extension $K/k$ of global fields with Galois group $G$, and a set $S$ of places of $K$ which is $G$-invariant, contains the infinite and the ramified primes, and is "large", which means that the $S$-class group of $K$ is trivial. In this setting, Tate constructed a class of 2-extensions with typical representative $0 \to U_S(K) \to P \to Q \to X_S \to 0$. Here $P$ is $G$-cohomologically trivial and $Q$ is $\mathbb{Z}[G]$-projective; $X_S$ is the kernel of augmentation on $Y_S$, the free $\mathbb{Z}$-module with basis $S$, and $U_S = U_S(K)$ is the group of $S$-units of $K$. The Yoneda class of this 2-extension is determined by local and global class field theory. For more details we refer the reader to [Ta].

These "Tate sequences" are extremely important in much of contemporary research in number theory, e.g. on leading term conjectures and their applications. But they continue to be somewhat elusive, since it is very hard to work back through all the necessary ingredients from local and global class field theory. In this note, we start from the observation that one can say a lot about the structure of Tate sequences just by algebraic methods. We use this to deduce lower bounds on the ranks of class groups. For totally real fields, these reprove results of Cornell–Rosen and earlier work of several authors. (A sharpening of these earlier results does not seem possible.) In the situation of CM fields, working in the minus part throughout, we retrieve and generalise results of R. Kučera and the author. Everything will be done $\ell$-adically, where $\ell$ is a fixed odd prime; this also means that we only look at $A(K)$, which is by definition the $\ell$-primary part of the class group $\mathrm{Cl}(K)$ of $K$. We make the further restrictive assumption that $G$ is an $\ell$-group, since this seems to be the most interesting case. Most of the time we will allow $G$ to be nonabelian.

2010 *Mathematics Subject Classification*: Primary 11R29.
*Key words and phrases*: Tate sequences, class groups, cohomology, totally real fields, CM fields.

DOI: 10.4064/aa160-1-4  

**2. "Identifying" the Tate sequence.** Recall that we always assume $G$ to be a finite $\ell$-group for a fixed prime $\ell$. The algebra $\Lambda = \mathbb{Z}_\ell[G]$ is then local, and $\Lambda$ is $\Lambda$-isomorphic to its $\mathbb{Z}_\ell$-linear dual. A *lattice* will mean a finitely generated $\Lambda$-module without $\mathbb{Z}_\ell$-torsion.

The Krull–Schmidt theorem holds over $\Lambda$: every lattice is the direct sum of indecomposable ones, uniquely up to isomorphism and ordering, and the endomorphism ring of every indecomposable lattice is local. There is a special class of lattices, the so-called *permutation lattices* $\mathbb{Z}_\ell[G/H]$, with $H \leq G$ any subgroup; they are all cyclic over $\Lambda$ and hence indecomposable.

There is *Heller's $\Omega$ operator*: given a lattice $M$, one takes a *free cover* $F \to M$ (that is, an epimorphism $f : F \to M$ such that $F$ is free over $\Lambda$ and $f$ maps a minimal set of generators of $F$ to a minimal set of generators of $M$), and sets $\Omega M = \ker(f)$. It is well known that $\Omega$ commutes with direct sums, and $\Omega M$ is nonfree indecomposable whenever $M$ is. Note that for the free indecomposable module $M = \Lambda$, we have $\Omega M = 0$. There are also the iterated Heller operators $\Omega^i$ for $i = 2, 3, \ldots$, and the inverse operators $\Omega^{-i} M = (\Omega^i M^*)^*$. (This latter construction uses the duality property mentioned in the first paragraph of this section; $M^*$ denotes the $\mathbb{Z}_\ell$-dual of $M$.) We will mainly be concerned with the operator $\Omega^2$, which is closely linked to the theory of Tate sequences. The initial stage of the following arguments can already be found, in a similar form, in [Ri, pp. 144 f.].

Schanuel's lemma states the following: If $F$ and $F_0$ are free and $f : F \to M$ and $f_0 : F_0 \to M$ are epimorphisms which are not necessarily covers, then $\ker(f_0) \oplus F$ is isomorphic to $\ker(f) \oplus F_0$. Thus the Heller operator $\Omega$ is also defined if one waives the requirement of $f$ being a cover, but this time only up to free direct summands. The same is true for the iterations $\Omega^i$: if we calculate up to free summands, then any free resolution of length $i$ will do. Let us state this explicitly for $\Omega^2$: Suppose $0 \to \Omega^2 M \to F' \to F \to M \to 0$ is a minimal free resolution of $M$, and $0 \to N \to F_1 \to F_0 \to M \to 0$ is another free resolution. Then $\Omega^2 M$ and $N$ become isomorphic after adding free summands to both of them. But by Krull–Schmidt and the fact that $\Omega^2 M$ has no nonzero free summands, we infer that $N \cong \Omega^2 M \oplus \tilde{F}$ for some free module $\tilde{F}$.

Now let us assume that $K$ does not contain any nontrivial $\ell$th roots of unity. The theory of Tate sequences produces a 2-extension

$$0 \to U \to A \to B \to X \to 0,$$

where $X = \mathbb{Z}_\ell \otimes X_S$ and $U = \mathbb{Z}_\ell \otimes U_S$; the modules $A$ and $B$ are free. (In general we only have $B$ projective and $A$ cohomologically trivial; but here $A$ has no torsion, so it is projective, and all projective modules over the local ring $\Lambda$ are free.) This 2-extension has a precisely specified class $c$ in $\mathrm{Ext}^2_\Lambda(X, U)$, and it induces isomorphisms on cohomology groups $\mathrm{H}^{q+2}(V, U) \to \mathrm{H}^q(V, X)$

for all $q \in \mathbb{Z}$ and all $V \leq G$. (We always use Tate cohomology in this paper.) Let us now look at a second 2-extension given by a 2-step minimal free resolution:

$$0 \to \Omega^2 X \to F' \to F \to X \to 0.$$

We remark already at this point that $X$ is completely explicit (very close to a direct sum of permutation lattices), so everything in this sequence can also been written down explicitly, at least in principle. Then we know, as explained above:

PROPOSITION 2.1. *$\Omega^2 X$ is isomorphic to a direct summand of $U$, and the complementary summand in $U$ is free.*

This is completely independent of knowing the class $c$. One can actually go much further (which we are not going to need in this note). Indeed, using work of Bley–Burns [BB] (Prop. 2.1) and of Holland [Ho] one can show:

THEOREM 2.2. *After changing the Tate sequence without changing its class $c$, there exists an injective morphism $\varphi : \Omega^2 X \to U = \mathbb{Z}_\ell U_S$ that represents $c$ under the identification $\mathrm{Ext}^2(X, U) \cong \mathrm{Hom}(\Omega^2, U)$. This map $\varphi$ gives rise to a pushout diagram*

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \Omega^2 X & \longrightarrow & F' & \longrightarrow & F & \longrightarrow & X & \longrightarrow & 0 \\ & & {\scriptstyle\varphi}\downarrow & & \downarrow & & {\scriptstyle=}\downarrow & & {\scriptstyle=}\downarrow & & \\ 0 & \longrightarrow & U & \longrightarrow & A & \longrightarrow & F & \longrightarrow & X & \longrightarrow & 0 \end{array}$$

*in which $U$ is the direct sum of $\varphi(\Omega^2 X)$ and a $\Lambda$-free complement.*

Already Proposition 2.1, which does not identify the map $\varphi$ via the canonical class, gives a lot of information on the $\ell$-adified Tate sequence, and this is all we are going to use.

**3. From Tate sequences to class number bounds.** We need a little notation. Let $I_G$ denote the augmentation ideal in $\mathbb{Z}[G]$. For any finitely generated $\Lambda$-module $M$ let $\mu(M)$ be the minimal number of generators of $M$. By Nakayama's lemma, this is the same as the $\mathbb{F}_p$-dimension of $M/\mathfrak{m}M$, where $\mathfrak{m} = p\Lambda + \mathbb{Z}_\ell I_G$ is the radical of the local ring $\Lambda = \mathbb{Z}_\ell[G]$. Let us assume until further notice that $K/k$ is ramified somewhere. Then we split up $S$ into the set $S_d$ of $k$-places that are totally decomposed in $K$ and the nonempty complement $S_0$. Let $r(k)$ denote the number of infinite places of $k$. If $\mathrm{Cl}(K)$ can be generated by $m$ elements as a $\mathbb{Z}[G]$-module, then one can always find $S$ such that $S_d$ has $r(k) + m$ elements: $r(k)$ to account for the places at infinity, and $m$ finite places which are totally split in $K/k$, such that each given generator of $\mathrm{Cl}(K)$ is the class of one of them, to make the set $S$ large. (This of course uses the theorem of Chebotarev.) Actually one does not quite need $S$ to be large for the existence of a Tate sequence;

it suffices to have the $S$-class group $G$-cohomologically trivial. A fortiori, it suffices that the $S$-class group has order prime to $\ell$. Thus we can find $S$ such that $S_d$ has $r(k) + \mu(A(K))$ elements (recall $A(K)$ is the $\ell$-part of $\mathrm{Cl}(K)$). Turning this around we find:

*Whenever we can establish a lower bound $B(K/k)$ on the cardinality of $S_d$, we get the lower bound $B(K/k) - r(k)$ for $\mu(A(K))$.*

This will be our program. Let $\mu_1(M)$ denote the minimal number of generators of $\Omega^1 M$, and let

$$\varepsilon(M) = \mu_1(M) - \mu(M)$$

for every finitely generated $\Lambda$-module $M$ (a kind of truncated Euler characteristic). In the following, rk denotes either $\mathbb{Z}$-rank or $\mathbb{Z}_\ell$-rank, depending on context. We note that $\mathrm{rk}(U_S) = \mathrm{rk}(X_S)$. In the minimal resolution used above to define $\Omega^2 X$ (recall $X = \mathbb{Z}_\ell \otimes X_S$) we have $\mathrm{rk}(F) = |G|\mu(X)$ and $\mathrm{rk}(F') = |G|\mu_1(X)$. The first inequality in the following chain uses the observation that $\Omega^2 X$ is a direct summand of $\mathbb{Z}_\ell \otimes U_S$ by Prop. 2.1:

$$\begin{aligned}\mathrm{rk}(U_S) \geq \mathrm{rk}(\Omega^2 X) &= |G|(\mu_1(X) - \mu(X)) + \mathrm{rk}(X)\\ &= |G| \cdot \varepsilon(X) + \mathrm{rk}(U_S).\end{aligned}$$

From these simple relations we infer the basic fact that

$$\varepsilon(X) \leq 0.$$

If we now let $X_0 = \mathbb{Z}_\ell X_{S_0}$ (the augmentation kernel on the free $\mathbb{Z}_\ell$-module $Y_0$ with basis $S_0(K)$), then $X$ splits up in the form $X = X_0 \oplus Y_{S_d(K)}$, and $Y_{S_d(K)}$ is $\Lambda$-free of rank $|S_d|$. Since $\varepsilon(\Lambda) = -1$ (note that $\Lambda$ needs one generator and $\Omega^1 \Lambda = 0$), and since $\varepsilon$ is certainly additive on direct sums, we find from the last inequality:

Proposition 3.1. *Whenever the set $S$ is large, then $|S_d| \geq \varepsilon(X_0)$.*

As a consequence we obtain

Theorem 3.2. *The quantity $\varepsilon(X_0) - r(k)$ is an a priori lower bound for $\mu(A(K))$.*

Remark. The module $X_0$ is not an invariant of the extension $K/k$: there is some ambiguity, but not too much. We have $X_0 = \mathbb{Z}_\ell X_{S_0}$, where $S_0$ *must* contain all ramified places, and it *may* contain some unramified but not totally split places. (The case $K/k$ unramified everywhere is special and will be discussed later.)

**4. Determining the bound.** Now we simply have to determine the number $\varepsilon(X_0)$, or at least find a good lower bound for it. After doing this in general, we will also consider minus parts in a CM situation, where things are considerably simpler, as the difference between the modules $X_S$ and

$Y_S$ disappears. The methods are very algebraic and standard, using the functors $\mathrm{Tor}_i^{\Lambda}(-,-)$. The supercript $\Lambda$ will usually be omitted, since most of our modules will be over $\Lambda$, and we further abbreviate:

$$\mathrm{Tor}_i(M) := \mathrm{Tor}_i(M, \mathbb{F}_\ell).$$

Then $\mathrm{Tor}_0(M) = M/\mathfrak{m}M$.

In what follows, dim will always mean $\mathbb{F}_p$-dimension.

LEMMA 4.1.

(a) $\dim \mathrm{Tor}_i(M) = \mu(\Omega^i M)$ *for all* $i \in \mathbb{N}$.
(b) $\varepsilon(M) = \dim \mathrm{Tor}_1(M) - \dim \mathrm{Tor}_0(M)$.

*Proof.* (a) We will only need this for $i = 0$, where the statement is clear, and for $i = 1$. (The other cases are also easy.) So let us prove the lemma for $i = 1$. Take a minimal resolution $0 \to N \to F \to M \to 0$. Then $\mathrm{Tor}_1(F) = 0$ since $F$ is free, and hence flat. We do not have $\mathrm{Tor}_0(F) = 0$, but by minimality of the resolution, the map

$$\mathrm{Tor}_0(N) = N/\mathfrak{m}N \to M/\mathfrak{m}M = \mathrm{Tor}_0(M)$$

is zero. So the long exact sequence for Tor gives $\mathrm{Tor}_1(M) \cong \mathrm{Tor}_0(N) = N/\mathfrak{m}N$. As $N = \Omega^1 M$, this proves what we want.

(b) This follows from (a) and the definition of $\varepsilon$. ∎

Now let $s(G)$ be the minimal number of generators of the group $G$. Note this is equal to the rank of the Frattini quotient of $G$, and also to $\mu(I_G)$. Recall that by definition we have a s.e.s. $0 \to X_0 \to Y_0 \to \mathbb{Z}_\ell \to 0$, and $Y_0$ is the direct sum of permutation modules $\mathbb{Z}_\ell[G/G_v]$, $v$ running over $S_0$. Let $C := \mathrm{coker}(\mathrm{Tor}_2(Y_0) \to \mathrm{Tor}_2(\mathbb{Z}_\ell))$, and define $\rho = \dim(C)$. We then have:

PROPOSITION 4.2. $\varepsilon(X_0) = \varepsilon(Y_0) - s(G) + 1 + \rho$.

*Proof.* Consider the exact sequence

$$0 \to C \to \mathrm{Tor}_1(X_0) \to \mathrm{Tor}_1(Y_0) \to \mathrm{Tor}_1(\mathbb{Z}_\ell) \\ \to \mathrm{Tor}_0(X_0) \to \mathrm{Tor}_0(Y_0) \to \mathrm{Tor}_0(\mathbb{Z}_\ell) \to 0.$$

This gives

$$\varepsilon(X_0) = \varepsilon(Y_0) - \varepsilon(\mathbb{Z}_\ell) + \rho.$$

But it is easy to determine $\varepsilon(\mathbb{Z}_\ell)$: its value is $s(G) - 1$ since $\mathrm{Tor}_0(\mathbb{Z}_\ell)$ is 1-dimensional and $\mathrm{Tor}_1(\mathbb{Z}_\ell) = \mathrm{Tor}_0(I_G)$ is $s(G)$-dimensional. ∎

It remains to deal with the right hand terms in Prop. 4.2. Let us start with $\varepsilon(Y_0)$; this is the sum $\sum_{v \in S_0} \varepsilon(\mathbb{Z}_\ell[G/G_v])$, and the $v$th summand is $s(G_v) - 1$, by a similar argument to the last proof. The hardest part is of course determining $\rho$.

For this we need to understand the terms $\mathrm{Tor}_2(\mathbb{Z}_\ell[G/G_v])$ (we recall that this is shorthand for $\mathrm{Tor}_2^{\mathbb{Z}_\ell[G]}(\mathbb{Z}_\ell[G/G_v], \mathbb{F}_\ell)$). Note that $\mathbb{Z}_\ell[G/G_v]$ can also be

seen as the induction of the trivial module $\mathbb{Z}_\ell$ from $G_v$ to $G$. We are going to link up the Tor groups with cohomology. It follows from the construction of homology and the universal property of the higher Tor's that $\mathrm{Tor}_2(M, \mathbb{Z}_\ell) = \mathrm{H}_2(G, M)$. This holds in particular for $M = \mathbb{Z}_\ell[G/V]$ with $V < G$ being any subgroup; by Shapiro's lemma, then, $\mathrm{H}_2(G, M) = \mathrm{H}_2(V, \mathbb{Z}_\ell)$. On the other hand, $\mathrm{H}_2(V, \mathbb{Z}_\ell)$ is functorially (in $V$) isomorphic to $\bigwedge^2 V^{\mathrm{ab}}$ (via $\mathrm{H}_2 \cong \mathrm{H}^{-3}$).

In a similar vein we get

$$\mathrm{Tor}_1(\mathbb{Z}_\ell[G/V], \mathbb{Z}_\ell) \cong \mathrm{H}_1(G, \mathbb{Z}_\ell[G/V]) \cong \mathrm{H}^{-2}(V, \mathbb{Z}_\ell) \cong V^{\mathrm{ab}}.$$

Actually it is tempting here to write $\bigwedge^1 V^{\mathrm{ab}}$ instead of $V^{\mathrm{ab}}$! We will soon put $V = G_v$ and take the direct sum over $v$.

The obvious short exact sequence $0 \to \mathbb{Z}_\ell \to \mathbb{Z}_\ell \to \mathbb{F}_\ell \to 0$ now gives a short exact sequence:

$$0 \to \mathrm{Tor}_2(\mathbb{Z}_\ell[G/V], \mathbb{Z}_\ell)/\ell \to \mathrm{Tor}_2(\mathbb{Z}_\ell[G/V], \mathbb{F}_\ell) \to \mathrm{Tor}_1(\mathbb{Z}_\ell[G/V], \mathbb{Z}_\ell)[\ell] \to 0.$$

(Here of course $\ldots/\ell$ means cokernel of multiplication by $\ell$, and $\ldots[\ell]$ means its kernel.) Rewriting the outer terms we get

$$(*) \qquad 0 \to \textstyle\bigwedge^2(V^{\mathrm{ab}}/\ell) \to \mathrm{Tor}_2(\mathbb{Z}_\ell[G/V], \mathbb{F}_\ell) \to V^{\mathrm{ab}}[\ell] \to 0.$$

The canonical map $\eta : \mathrm{Tor}_2(Y_0, \mathbb{F}_\ell) \to \mathrm{Tor}_2(\mathbb{Z}_\ell, \mathbb{F}_\ell)$ now arises from taking $V = G_v$ for each $v \in S_0$ in $(*)$, using functoriality via the inclusions $G_v \subset G$, and taking the direct sum over $v$ of all the resulting maps $\mathrm{Tor}_2(\mathbb{Z}_\ell[G/G_v], \mathbb{F}_\ell) \to \mathrm{Tor}_2(\mathbb{Z}_\ell[G/G], \mathbb{F}_\ell) = \mathrm{Tor}_2(\mathbb{Z}_\ell, \mathbb{F}_\ell)$. We want to show that $\eta$ can actually be described in more explicit terms. It is clear that the restriction of $\eta$ to the respective left hand terms in the s.e.s. $(*)$ is well defined, and gives the natural map $\eta^+$ (say) : $\bigoplus_v \bigwedge^2 G_v^{\mathrm{ab}}/\ell \to \bigwedge^2 G^{\mathrm{ab}}/\ell$ that was already studied by several authors, for example Cornell and Rosen. It is likewise clear that $\eta$ induces a map $\eta^-$ on the right hand terms of $(*)$, which is again the natural map $\bigoplus_v G_v^{\mathrm{ab}}[\ell] \to G^{\mathrm{ab}}[\ell]$. But we want to understand the entire map $\eta$; remember that we need the dimension of its cokernel $C$.

Fortunately, since $\ell > 2$, it will be possible to split up $\eta$ into $\eta^+$ and $\eta^-$ in a functorial way. We claim that inversion of group elements induces an automorphism $\iota$ on all Tor groups involved. It is clear that inversion induces the identity on the left hand term $\bigwedge^2(V^{\mathrm{ab}}/\ell)$ in $(*)$, and minus identity on the right hand term $V^{\mathrm{ab}}[\ell]$ in $(*)$. (It would not even be necessary to take the cokernel and kernel of $\ell$ respectively.) The main point to show is that inversion of group elements induces *some* automorphism $\iota$ of the middle term $\mathrm{Tor}_2(\mathbb{Z}_\ell[G/V], \mathbb{F}_\ell)$ in $(*)$ in a natural way. First we identify this middle term with $\mathrm{H}_2(V, \mathbb{F}_\ell)$. (We briefly explain this identification. First, an easy spectral sequence argument shows that

$$\mathrm{Tor}_2^{\mathbb{Z}_\ell[G]}(\mathbb{Z}_\ell[G/V], \mathbb{F}_\ell) = \mathrm{Tor}_2^{\mathbb{Z}_\ell[V]}(\mathbb{Z}_\ell, \mathbb{F}_\ell).$$

The main point in this is that the forgetful functor from $G$-modules to $V$-modules is exact and takes projectives to projectives. Second, $\mathrm{Tor}_*^{\mathbb{Z}_\ell[V]}(\mathbb{Z}_\ell, M)$ is the left-derived functor of $M \mapsto \mathbb{Z}_\ell \otimes_{\mathbb{Z}_\ell[V]} M$, and $\mathrm{H}_*(V, M)$ is the left-derived functor of $M \mapsto M_V$; since $M_V$ is nothing else but $\mathbb{Z}_\ell \otimes_{\mathbb{Z}_\ell[V]} M$, these two derived functors are canonically identified, and we just have to put $M = \mathbb{F}_\ell$.) If $V$ is abelian, then inversion on $V$ and identity on the trivial $V$-module $\mathbb{F}_\ell$ induce the desired involution $\iota$. (Compare the general discussion of functoriality of (co)homology on pp. 45 ff. of [NSW].) We now reduce to the case that $V$ is abelian. Let $\pi : V \to V^{\mathrm{ab}}$ be the canonical group epimorphism. Then $\pi$ and $\mathrm{id}_{\mathbb{F}_\ell}$ define a morphism $\pi_* : \mathrm{H}_2(V, \mathbb{F}_\ell) \to \mathrm{H}_2(V^{\mathrm{ab}}, \mathbb{F}_\ell)$. (Note the arrow is indeed going this way; in [NSW] we have a reversal of direction, but there cohomology is discussed, not homology.) Now by looking at two copies of the short exact sequence $(*)$, one for $V$ and one for $V^{\mathrm{ab}}$, and by the 5-lemma, one sees that $\pi_*$ is an isomorphism. This shows that the involution $\iota$ (arising from inversion of group elements) exists on homology, even if $V$ is not abelian.

As we said, $\iota$ acts as identity on all terms $\bigwedge^2 G_v^{\mathrm{ab}}$, and as minus identity on all terms $G_v^{\mathrm{ab}}$. Hence all sequences $(*)$ with $V = G_v$ split functorially, and $\mathrm{coker}(\eta)$ is the direct sum of $\mathrm{coker}(\eta^+)$ (the cokernel studied by Cornell–Rosen et al.), and of $\mathrm{coker}(\eta^-)$, which is a much simpler object. Let $\rho^\pm$ be the dimension of $\mathrm{coker}(\eta^\pm)$.

By combining Theorem 3.2 with Proposition 4.2 and the discussion following it, we end up with the following result (let us repeat all our hypotheses for the sake of clarity):

THEOREM 4.3. *Suppose $\ell$ is a fixed odd prime and $K/k$ is a Galois $\ell$-extension of global fields, which is ramified somewhere. Assume that $K$ contains no $\ell$th root of unity. Then we have the following lower bound on the number of Galois generators of the $\ell$-part of the class group of $K$:*

$$\mu(A(K)) \geq \sum_{v \in S_0} (s(G_v) - 1) + 1 - s(G) + \rho^+ + \rho^- - r(k).$$

*Here $r(k)$ is the number of infinite places of $k$, and the nonnegative integers $\rho^+, \rho^-$ are defined above.*

It is not hard to see exactly when the inequality of the theorem is an equality. It suffices to go back to §2; to be consistent with §2 we have to assume that $S$ is the disjoint union $S_0 \cup S_\infty \cup \{v_1, \ldots, v_\mu\}$, where the $v_i$ are totally split primes, whose classes are a minimal generating set of $\mathrm{cl}(K)\{\ell\}$. Now in all inequalities of §2, the difference between the larger and the smaller term is $f(\mathbb{Z}_\ell \otimes U_S)$, which is defined as the rank of the $\Lambda$-free part of $\mathbb{Z}_\ell \otimes U_S = U$. Thus we have equality in the above theorem iff $U$ has no nontrivial

$\Lambda$-free summand. In other words, we have $U \cong \Omega^2 X$ in this case. If $\Omega^2 X$ is itself indecomposable, then so is $U$ in this case.

As an example take $k = \mathbb{Q}$ and $K$ a bicyclic tame extension of degree $\ell^2$. Then exactly two primes $p_1$ and $p_2$ are ramified, both congruent 1 modulo $\ell$. If we further assume that both of the $p_i$ have nontrivial inertia, then $\ell$ does not divide $h_K$ (see next paragraph), and one can also check that the right hand side in the theorem is zero (hence equality in the theorem). So $S = S_0 \cup S_\infty$, and one quickly calculates that $X \cong \mathbb{Z}_\ell[G] \oplus \mathbb{Z}_\ell$; therefore

$$U \cong \Omega^2 X = \Omega^2 \mathbb{Z}_\ell.$$

One can write down an explicit presentation for the latter module, and compare it directly with an explicit presentation for $U$ coming from cyclotomic units. In detail (of course the reader is welcome to skip this, and we are not claiming this is new): let $\sigma, \tau$ be generators of $G = \mathrm{Gal}(K/\mathbb{Q})$ such that the fixed field of $\sigma$ (resp. $\tau$) is the cyclic subfield $K_1$ (resp. $K_2$) of conductor $p_1$ (resp. $p_2$). Here $\Omega^2 X \subset \Lambda^2$ is generated by three elements: $\omega_1 = (N_\sigma, 0)$, $\omega_2 = (0, N_\tau)$, and $\omega' = (\tau - 1, 1 - \sigma)$. Then $\omega'$ corresponds to the "conductor-level" cyclotomic unit in $K$; $\omega_i$ corresponds to the standard cyclotomic $p_i$-unit belonging to $K_i$ $(i = 1, 2)$. The obvious relations between these three elements of $\Omega^2 X$ just mirror the Euler relations between cyclotomic numbers.

After these side remarks, let us now look at a family of fields that was also studied by Cornell and Rosen in [CR]. Let $G$ be $\ell$-elementary of rank $m$ (hence of order $\ell^m$), and let $K/\mathbb{Q}$ be $G$-Galois and (totally) real. Then $G$ is generated by the $G_v$ with $v$ ramified, so $\rho^-$ is zero. On the other hand, $\rho^+$ is exactly the quantity which Cornell and Rosen show to be equal to the $\ell$-rank of the "central class group" of $K$ over its genus field (see [CR, p. 457]). As $k = \mathbb{Q}$, the right hand side in the theorem is

$$\sum_{v \in S_0} (s(G_v) - 1) - m + \rho^+.$$

It is known that the $\ell$-rank of the central class field equals the minimal number of generators of the class group. So if $K$ is its own genus field, the result in [CR] says exactly $\mu(A(K)) \geq \rho^+$. Our term $(s(G_v) - 1) - m$ is in that case never positive, since every term $s(G_v) - 1$ is either 1 or 0, and there are $m$ terms. Its value is $-m'$, where $m'$ is the number of primes $p_i$ having trivial inertia. That is: our result is a little weaker than the one in [CR] in general. However, $\rho^+$ is hard to evaluate; Cornell and Rosen consider the obvious lower bound $m(m-1)/2 - m = m(m-3)/2$. (Here $m(m-1)/2$ is the dimension of $\bigwedge^2 G$, and every $\bigwedge^2 G_v$ is at most one-dimensional.) But we can replace this lower bound by $m(m-1)/2 - (m - m')$, since $\bigwedge^2 G_{p_i} = 0$ if $p_i$ has no inertia. Hence our lower bound also comes out as

$m(m-1)/2-(m-m')-m'=m(m-1)/2-m$, and this is exactly the explicit bound given by Cornell and Rosen.

This class of examples can be generalised to any base field $k$; in the above formula one has to add the extra term $1-r(k)$. The resulting bound could also be deduced from [CR], using work of Furuta as well (see [Fu], in particular eqn. (7)). Our approach is less involved, once one accepts the existence and standard properties of Tate sequences, and it says a lot about the Galois module structure of units.

We finish this section with some remarks on the case where $K/k$ is everywhere unramified. Then we can take $S$ to consist of $\mu(A(K))+r(k)$ places of $k$ which are totally split in $K$. We pick one $v_0\in S$ and let $S_d=S\setminus\{v_0\}$, so $S_0=\{v_0\}$. Then $X_0$ is defined as before, but here it is easy to grasp: it is isomorphic to the augmentation ideal in $\mathbb{Z}_\ell[G]$. As before, we have $|S_d|\geq\varepsilon(X_0)$ and hence $\mu(A(K))\geq\varepsilon(X_0)-r(k)+1$. On the other hand we can determine $\varepsilon(X_0)$ exactly. One can either use the approach described above (involving $\rho$), but for a change we can also say that it is well known from a kind of bar resolution that $X_0\cong\mathbb{Z}_\ell I_G$ requires $s(G)$ generators, and the first syzygy $\Omega^1(X_0)$ requires $s(G)(s(G)+1)/2$ generators, so $\varepsilon(X_0)=s(G)(s(G)-1)/2$. We end up with the bound

$$\mu(A(K))\geq\frac{s(G)(s(G)-1)}{2}+1-r(k).$$

Whilst this lower bound seems to be far too weak to produce infinite class field towers because $r(k)$ grows too quickly, it is easy to obtain some explicit results; we give two examples. Assume $k$ is imaginary quadratic and the class group of $k$ has $\ell$-rank 2. (For $\ell=3$ one can take $k=\mathbb{Q}(\sqrt{-4027})$.) So we get an $\ell$-elementary unramified extension $K/k$ of degree $\ell^2$, that is, $s(G)=2$. Our bound then says that the $\ell$-rank of $\mathrm{Cl}(K)$ is at least $2\cdot 1/2+1-1=1$. The same holds if one replaces $K$ by the full Hilbert 3-class field of $k$, or the full Hilbert class field. (With specialised methods one can show more: generalising work of Scholz and Taussky, Arrigoni [Ar] proves that the $\ell$-rank in question is at least 3.) Now take $k$ imaginary quadratic such that the $\ell$-rank of the class group is 5. (Example for $\ell=3$: $k=\mathbb{Q}(\sqrt{-5393946914743})$.) Then $k$ has an $\ell$-elementary unramified extension $k$ of degree $\ell^5$, and our bound shows that the $\ell$-rank of $\mathrm{Cl}(K)$ is at least $5\cdot 4/2+1-1=10$. As the reader can see, our bound does not allow us to continue in either case, since the term $r(K)$ is too big. At least in the first case discussed above, this fits with reality: Arrigoni demonstrates that it is possible for the $\ell$-class field tower to be finite. In the second case it is unsatisfactory since one knows for odd $\ell$ and imaginary quadratic $k$ that if the $\ell$-rank of $\mathrm{Cl}(K)$ is at least 3, then the $\ell$-class field tower is infinite. (See [Sch].)

**5. The CM case.** We assume here that $k$ is a totally real number field, and $K$ is CM (a totally imaginary extension of a totally real number field $K^+$). Then $\mathrm{Gal}(K/k)$ contains a unique, central element $j$ inducing complex conjugation on $K$ (whatever the embedding into $\mathbb{C}$). For the sake of simplicity let us assume that the Galois group of $K/k$ splits as $\{1,j\}\times G$, with $G$ an $\ell$-group. Note that this involves a slight change in the meaning of the letter $G$. For every $\mathrm{Gal}(K/k)$-module $M$ on which 2 acts invertibly, we let $M^-$ be the kernel of $1+j$ on $M$, as is customary. We call $M^-$ the *minus part* of $M$; taking the minus part is an exact functor. Let $U = \mathbb{Z}_\ell \otimes U_S(K)^-$ and $X = \mathbb{Z}_\ell \otimes X_S$, just as before.

There are minus versions of the results in the earlier sections. Let $S^*$ be the subset of $S$ consisting of those places $v$ not having $j$ in their decomposition group, and let $S_d^* = S^* \cap S_d$, $S_0^* = S^* \cap S_0$. Then $X^-$ is isomorphic to $Y_{S^*}^-$ (the effect of taking the augmentation kernel disappears in the minus part), and if we let $X_0^- = X_{S_0^*}^- = Y_{S_0^*}^-$, then $X^-$ is the direct sum of $X_0^-$ and a free $\mathbb{Z}_\ell[G]$-module of rank $|S_d^*|$ (on which $j$ acts as $-1$). It is now very important to note that $S^*$ contains no infinite place. There is also the module $X_{\mathrm{ram}} := X_{S_{\mathrm{ram}}}$ and its minus part, where $S_{\mathrm{ram}}$ denotes the set of finite places of $k$ which ramify in $K$.

We now obtain an analog of Theorem 2.1 in the minus part. Note that the term $-r(k)$ has disappeared.

THEOREM 5.1. *The quantity $\varepsilon(X_{\mathrm{ram}}^-)$ is a lower bound for $\mu(A(K)^-)$. (Note that $X_{\mathrm{ram}}^- = Y_{S_{\mathrm{ram}}}^-$.)*

*Proof.* Suppose $A(K)^-$ is minimally gerated by $m$ elements. We try to imitate the proof of 3.1, asking ourselves how many places have to go into a large set $S$. We certainly need $S_\infty \cup S_{\mathrm{ram}} \subset S$. In contrast to the proof of 3.1, it will not suffice to put in a set $S_d$ of $m$ totally split finite places, one place for each generator of $A(K)^-$; we need more places in $S$ to get rid of $A(K)^+$ as well. By Chebotarev and the fact that $K/K^+$ is ramified (at infinity), we see that for each element $x$ of $A(K)^+$ one can find a prime $\mathfrak{P}_x$ of $K^+$ that stays inert in $K$ and represents $x$. We let $\mathfrak{p}_x$ be the prime of $k$ below $\mathfrak{P}_x$ and $S'$ be the set of all these $\mathfrak{p}_x$ with $x$ running through a set of generators of $A(K)^+ = A(K^+)$. Now we put

$$S = S_d \cup S' \cup S_{\mathrm{ram}} \cup S_\infty.$$

Only the places in $S_d$ are totally split, so $S_0 = S' \cup S_{\mathrm{ram}} \cup S_\infty$. The same reasoning as in the proof of 3.1 (with appropriate exponents "minus") shows that $|S_d| = m \geq \varepsilon(X_{S_0}^-)$. But no places in $S'$ and in $S_\infty$ are in $S^*$ (i.e., split from $K^+$ to $K$), and hence $X_{S_0}^- = X_{\mathrm{ram}}^-$. ∎

Now $\varepsilon(X_{\mathrm{ram}}^-)$ is much easier to calculate than without the minus sign. By definition, the decomposition group $G_v$ of any $v \in S^*$ is contained in $G$

(which is the $\ell$-part of $\mathrm{Gal}(K/k)$), and we get

$$X_{\mathrm{ram}}^{-} = Y_{S_{\mathrm{ram}}}^{-} = \bigoplus_{v \in S_{\mathrm{ram}}^{*}} \mathbb{Z}_\ell[G/G_v].$$

We already calculated $\varepsilon$ of these permutation modules. Indeed, we found that $\varepsilon(\mathbb{Z}_\ell[G/G_v]) = s(G_v) - 1$. Thus we get:

THEOREM 5.2. *Under the assumptions described above, we have*

$$\mu(A(K)^{-}) \geq \sum_{v \in S_{\mathrm{ram}}^{*}} (s(G_v) - 1).$$

Again, this gives in certain special situations a somewhat weaker version of a known result, this time a considerably more recent one than quoted from [CR] in §3). To wit, in [GK] we considered the following setup: $k = \mathbb{Q}$ and $K = FK_1 \dots K_s$, where $F/\mathbb{Q}$ is imaginary quadratic, and every $K_i$ is cyclic of degree $\ell$ over $\mathbb{Q}$, with conductor $p_i \equiv 1$ modulo $\ell$, and all $p_i$ are distinct and split in $F$. It is proved in [GK] that $\mathrm{cl}(K)\{\ell\}^{-}$ needs at least $s$ generators as a Galois module. Our present result is weaker in that setting since the right hand sum in Theorem 5.2 is exactly the number of $p_i$ with nontrivial inertia in $K/\mathbb{Q}$, hence at most $s$. (Recall that decomposition groups cannot require more than two generators in this tame absolutely abelian situation with $\ell$-elementary Galois group, and they are cyclic iff there is not both ramification and inertia.) But the theorem just above applies not only to this special kind of absolutely abelian situation.

**Acknowledgments.** The author would like to thank his audiences at Oujda (Morocco) and Waseda (Japan) for their valuable input, and the referee for his helpful report.

## References

[Ar] M. Arrigoni, *On Schur $\sigma$-groups*, Math. Nachr. 192 (1998), 71–89.

[BB] W. Bley and D. Burns, *Explicit units and the equivariant Tamagawa number conjecture*, Amer. J. Math. 123 (2001), 931–949.

[CR] G. Cornell and M. Rosen, *The class group of an absolutely Abelian $l$-extension*, Illinois J. Math. 32 (1988), 453–461.

[Fu] Y. Furuta, *On class field towers and the rank of ideal class groups*, Nagoya Math. J. 48 (1972), 147–157.

[GK] C. Greither and R. Kučera, *Annihilators of minus class groups for imaginary abelian fields*, Ann. Inst. Fourier (Grenoble) 57 (2007), 1623–1653.

[Ho] D. Holland, *Homological equivalences of modules and their projective invariants*, J London Math. Soc. 43 (1991), 396–411.

[NSW] J. Neukirch, A. Schmidt and K. Wingberg, *Cohomology of Number Fields*, 2nd ed., Springer, 2008.

[Ri] J. Ritter, *L-values at zero and the Galois structure of global units*, in: Algebra. Some Recent Advances, I. B. S. Passi (ed.), Trends Math., Birkhäuser, 1999, 135–169.

[Sch] R. Schoof, *Infinite class field towers of quadratic fields*, J. Reine Angew. Math. 372 (1986), 209–220.

[Ta] J. Tate, *Les conjectures de Stark sur les fonctions L d'Artin en s = 0*, Progr. Math. 47, Birkhäuser, 1984.

Cornelius Greither
Fakultät Informatik
Universität der Bundeswehr München
85577 Neubiberg, Germany
E-mail: cornelius.greither@unibw.de

*Received on 29.11.2012*
*and in revised form on 10.5.2013* (7272)