On torsion of class groups of CM tori

Article

Accepted Version

Daw, C. ORCID: https://orcid.org/0000-0002-2488-6729 (2012) On torsion of class groups of CM tori. Mathematika, 58 (2). pp. 305-318. ISSN 2041-7942 doi: https://doi.org/10.1112/S0025579312000022 Available at https://centaur.reading.ac.uk/70356/

Published version at: https://www.cambridge.org/core/journals/mathematika/article/on-torsion-of-class-groups-of-cm-tori/A84E096FEF0ACBAE3295710E67738257
To link to this article DOI: http://dx.doi.org/10.1112/S0025579312000022

Publisher: Cambridge University Press

On torsion of class groups of CM tori.

Christopher Daw *

May 15, 2017

Abstract

Let T be an algebraic torus over $\mathbb{Q}$ such that $T(\mathbb{R})$ is compact. Assuming the Generalised Riemann Hypothesis, we give a lower bound for the size of the class group of T modulo its n-torsion in terms of a small power of the discriminant of the splitting field of T. As a corollary, we obtain an upper bound on the n-torsion in that class group. This generalises known results on the structure of class groups of CM fields.

1 Introduction.

This paper is motivated by Zhang's "ϵ-conjecture", found in [11], proposing that the size of n-torsion in the class groups of CM fields of fixed degree grows slower than any positive power of the discriminant:

Conjecture 1.1 (ϵ-conjecture) *Fix a totally real number field F and a positive integer n. Then, for any real $\epsilon > 0$, there exists a constant $C(\epsilon)$ such that, for any quadratic CM extension L and any order $\mathcal{O}$ of L containing the ring of integers of F, the n-torsion of the class group of $\mathcal{O}$ has the following bound:*

$$\#Pic(\mathcal{O})[n] \leq C(\epsilon)\, disc(\mathcal{O})^{\epsilon}.$$

Recent results on torsion of the class groups of number fields, due to Ellenberg and Venkatesh, can be found in [3].

*University College London, Department of Mathematics, Gower Street, London WC1E 6BT, United Kingdom, email: c.daw@ucl.ac.uk

Understanding n-torsion in the class groups of CM tori arises as a natural problem in the study of Shimura varieties. In particular, it is part of several strategies for proving the André-Oort conjecture. The Galois action on special points of Shimura varieties is given by reciprocity morphisms of CM tori. To give a lower bound for the size of the orbits, one needs to bound the size of the images of the induced maps on class groups. Lower bounds for the size of class groups modulo n-torsion yield estimates on these quantities (see [6] and [7] for further details). Our results are primarily of this form.

Note that the Mumford-Tate group of a CM point is a CM torus. We work in the slightly more general setting of algebraic tori over $\mathbb{Q}$ whose real points are compact. Their splitting fields are CM fields. Let $\mathbb{A}_f$ denote the finite adeles over $\mathbb{Q}$. For an arbitrary algebraic torus M over $\mathbb{Q}$, we denote by K_M^m the maximal compact open subgroup of $M(\mathbb{A}_f)$. For any such torus we denote by h_M its class group i.e.

$$h_M = M(\mathbb{Q})\backslash M(\mathbb{A}_f)/K_M^m.$$

Given any $n \in \mathbb{N}$ we denote by $h_M[n]$ the n-torsion. For an arbitrary number field F, we denote by Δ_F the absolute value of the discriminant of F. Assuming the Generalised Riemann Hypothesis for CM fields we obtain the following bound.

Theorem 1.2 *Assume the Generalised Riemann Hypothesis for CM fields. Let T be an algebraic torus over $\mathbb{Q}$ of dimension d, with splitting field L, such that $T(\mathbb{R})$ is compact. Then we have*

$$|h_T/h_T[n]| \gg_{\epsilon,d} \Delta_L^{\frac{c}{2n}+\epsilon},$$

for all $\epsilon > 0$, where c is a positive constant depending only on d.

By splitting field we refer to the smallest field over which T becomes a product of copies of $\mathbb{G}_m$. Our method relies on the fact that T is isogenous to a product $T_1 \times \cdots \times T_s$ of simple tori. We fix surjective maps with connected kernels from $R := \mathrm{Res}_{L/\mathbb{Q}}\mathbb{G}_{m,L}$ to each of the T_i and take r to be the product of these surjections followed by an isogeny to T. For a prime p, split in L, $R(\mathbb{Q}_p)$ is isomorphic to the cocharacter group of R tensored with $\mathbb{Q}_p^*$. We use GRH to find small split primes and take an arbitrary product of powers of uniformisers lying over these primes in $R(\mathbb{A}_f)$. After projection to the factors $R(\mathbb{Q}_p)$, for each such prime p, these elements are permuted by

Gal($L/\mathbb{Q}$) over a basis for the cocharacter group. We embed these elements diagonally into the product of the $R(\mathbb{A}_f)$ and assume that this lies in the kernel of the map induced by r on class groups i.e. the image under r is an element $\pi k \in T(\mathbb{Q})K_T^m$. The element π gives us elements π_i in the $T_i(\mathbb{Q})$. We show that L is generated over $\mathbb{Q}$ by the images of the π_i under bases for the character groups of the T_i. We make them integral, scaling them by the primes p raised to the absolute values of the exponents of the uniformisers. We may take a basis for L over $\mathbb{Q}$ in terms of these elements, whose $\mathbb{Z}$-span is an order in $\mathcal{O}_L$, the ring of integers, which relates Δ_L to the absolute values of images of the π_i and their Galois conjugates. However, these absolute values are controlled by the primes found under GRH, a uniform bound on the character bases, and the exponents of the uniformisers. Since these primes are 'small', compared to Δ_L, we are able to bound the exponents from below. A group theoretic argument converts this into a lower bound for the size of the class group modulo n-torsion.

Our method relies crucially on the assumption that $T(\mathbb{R})$ is compact. However, note that, whilst the class group of a CM field L is the class group of the torus $R_L := \mathrm{Res}_{L/\mathbb{Q}}\mathbb{G}_m$, whose real points are not compact, this torus lies in an exact sequence

$$1 \to M \to R_L \to \mathbb{G}_m \to 1,$$

where M is a torus over $\mathbb{Q}$ whose real points are compact. Its $\mathbb{Q}$-points are precisely the elements of L of norm 1. This exact sequence of tori induces a morphism of class groups

$$h_M \to h_{R_L},$$

whose kernel has order bounded in terms of d only by [6], Theorem 5.1. We have another induced morphism from h_{R_L} to $h_{\mathbb{G}_m} = 1$. Again by Theorem 5.1. of [6], we deduce that

$$\frac{|h_{R_L}|}{|h_T|} \ll_{n_L,\epsilon} \Delta_L^{\epsilon},$$

for any $\epsilon > 0$, where $n_L = [L : \mathbb{Q}]$. Since we have a morphism

$$h_T[n] \to h_{R_L}[n],$$

with uniformly bounded kernel, for any $n \in \mathbb{N}$, Theorem 1.2 applies to CM fields and, indeed, to any extension of a suitable torus by a product of copies of $\mathbb{G}_m$.

The author is indebted to Andrei Yafaev for explaining his ideas on this subject and, more generally, for his indefatigable guidance and patience. The author is also grateful to the department of mathematics at UCL for their generosity this past year and to the referee for many helpful remarks regarding the presentation.

2 Corollary on n-torsion.

Before proceeding to the proof of Theorem 1.2 we give an implied upper bound on the size of n-torsion. All that is required is a simple upper bound on the class group of T. We have the following theorem.

Theorem 2.1 *Let T be an algebraic torus over $\mathbb{Q}$, with dimension d and splitting field L. Then we have*

$$|h_T| \ll_{\epsilon,d} \Delta_L^{\frac{s}{2}+\epsilon},$$

for all $\epsilon > 0$, where s is the number of simple subtori of T.

Proof. Proposition 2.1. of [4] ensures that we can put T into the exact sequence

$$1 \to T \to R_L^s \to M \to 1,$$

where M is a $\mathbb{Q}$-torus. Theorem 5.1. of [6] ensures that the induced map on class groups

$$h_T \to h_{R^s}$$

has kernel of uniformly bounded order and the class group h_{R^s} is simply the s-fold direct product of the class group $Cl(L)$ of L. By (1) of [2] we have

$$|Cl(L)| \ll_{\epsilon,n_L} \Delta_L^{\frac{1}{2}+\epsilon},$$

where n_L is the degree of L over $\mathbb{Q}$. We will later demonstrate that n_L is bounded in terms of d only, which completes the proof. □

The combination of Theorems 2.1 and 1.2 yield the following bound on the size of n-torsion in the class group.

Theorem 2.2 *Assume the Generalised Riemann Hypothesis for CM fields. Let T be an algebraic torus over $\mathbb{Q}$ of dimension d, with splitting field L, such that $T(\mathbb{R})$ is compact. Then we have*

$$|h_T[n]| \ll_{\epsilon,d} \Delta_L^{\frac{s}{2}-\frac{c}{2n}+\epsilon},$$

for all $\epsilon > 0$, where c is a positive constant depending only on d and s is the number of simple subtori of T.

3 A group theoretic argument.

The proof of theorem 1.2 will combine the ideas of two papers, [1] and [10]. Following [1], for an arbitrary Abelian group G and $l \in \mathbb{N}$, let $\mathcal{M}_G(l)$ be the smallest integer A such that for any l elements $g_1, ..., g_l \in G$, not necessarily distinct, there exist $a_1, ..., a_l \in \mathbb{Z}$, not all zero, with $\sum_{i=1}^{l} |a_i| \leq A$, such that

$$g_1^{a_1} \cdots g_l^{a_l} = 1.$$

In what follows we will demonstrate the following:

$$\mathcal{M}_{h_T}(l) > \frac{c \log \Delta_L}{\log(l) + \log\log \Delta_L}, \tag{1}$$

for any $l \in \mathbb{N}$, provided Δ_L is greater than a constant depending only on d. Here we prove that inequality (1) implies Theorem 1.2.

Proof. We follow the proof of Lemma 5.1. of [1]. Let G be a finite Abelian group, set $l = |G|$, and take $g_1, ..., g_l \in G$. If $g_i = 1$ for some $i \in \{1, ..., l\}$ then we clearly have a nontrivial relation between the g_i and so $A = 1$ with A defined as it was above. Otherwise, an element of G appears twice amongst our g_i and there exist i and j such that $i \neq j$ and $g_i g_j^{-1} = 1$. Either way, we have a nontrivial relation with $A \leq 2$. Hence, we have shown that

$$\mathcal{M}_G(|G|) \leq 2.$$

Henceforth, let $G = h_T/h_T[n]$. Then, by Lemma 5.1. (iii) of [1], we have

$$\mathcal{M}_{h_T}(|G|) \leq n\mathcal{M}_G(|G|)$$

and, therefore, by the preceeding argument,

$$\mathcal{M}_{h_T}(|G|) \leq 2n.$$

Substituting $\mathcal{M}_{h_T}(|G|)$ into (1), we obtain the desired result

$$l = |h_T/h_T[n]| > \frac{\Delta_L^{\frac{c}{2n}}}{\log \Delta_L},$$

provided $\Delta_L > 2$. □

The remainder of this paper is devoted to the proof of (1).

4 Covering T.

For an arbitrary algebraic torus M over $\mathbb{Q}$, we denote by $X^*(M)$ its character group i.e. the free $\mathbb{Z}$-module $\mathrm{Hom}(M_{\overline{\mathbb{Q}}}, \mathbb{G}_{m,\overline{\mathbb{Q}}})$ with the natural Galois action. The corresponding representation

$$\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to GL(X^*(M)),$$

has kernel $\mathrm{Gal}(\overline{\mathbb{Q}}/F)$, for some finite, Galois extension F, which we refer to as the *splitting field* of M.

We denote by $X_*(M)$ the group of cocharacters of M, by which we refer to the $\mathbb{Z}$-module $\mathrm{Hom}(\mathbb{G}_{m,\overline{\mathbb{Q}}}, M_{\overline{\mathbb{Q}}})$, again assuming a $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-action in the natural way, also factoring through $\mathrm{Gal}(F/\mathbb{Q})$. There is a natural bilinear map

$$X_*(M) \times X^*(M) \to \mathbb{Z},$$

identifying $X_*(M)$ with the dual $\mathbb{Z}[\mathrm{Gal}(F/\mathbb{Q})]$-module $\mathrm{Hom}(X^*(M), \mathbb{Z})$ of $X^*(M)$.

Recall that we have a semisimple category whose objects are algebraic tori and whose morphisms are the usual homomorphisms of algebraic tori (which form an abelian group) tensored with $\mathbb{Q}$. Therefore, our given T is isogenous to a product of tori $T_1 \times \cdots \times T_s$, where the T_i are simple i.e. they contain no proper subtori. Each T_i splits over a Galois extension L_i and the compositum of these fields is L. Two algebraic tori are isogenous precisely when their character groups are isomorphic when tensored with $\mathbb{Q}$.

Consider the torus $\mathrm{Res}_{F/\mathbb{Q}}\mathbb{G}_{m,F}$, derived from the multiplicative group $\mathbb{G}_{m,F}$ over a number field F by restriction of scalars to $\mathbb{Q}$. Tori of this form, along with their finite direct products, are often called *quasisplit*. They are characterised by the property that their character groups are permutation modules with respect to their Galois action. For example, the character group of R_L is $\mathbb{Z}[\mathrm{Gal}(L/\mathbb{Q})]$. In this regard, these tori are the easiest to study. We will make use of their tractability via the following special case of a general result (Proposition 2.2.) found in [4].

Lemma 4.1 *Let M be a simple algebraic torus over $\mathbb{Q}$, split over a Galois field F. Then M can be covered by the quasisplit torus*

$$R_F := Res_{F/\mathbb{Q}}\mathbb{G}_{m,F}.$$

That is, M can be put into an exact sequence

$$1 \to N \to R_F \to M \to 1,$$

where N is a $\mathbb{Q}$-torus.

Proof. The fact that M may be covered by some finite product R_F^l is Proposition 2.2. of [4]. However, since the Hom functor commutes with products, an element of

$$\mathrm{Hom}(R_F^l, M)$$

is a product of morphisms into M, each of which has an image constituting a subgroup of M. Since M is simple, all but one of these images must be trivial i.e. we may assume $l = 1$. □

In light of this, each T_i may be covered by a copy of R_L. Any such morphism of tori is equivalent to an injection of character groups

$$\xi : X^*(T_i) \hookrightarrow X^*(R_L).$$

We have proved the existence of such embeddings, but have not specified one precisely. We identify $X^*(R_L)$ with $\mathbb{Z}[\mathrm{Gal}(L/\mathbb{Q})]$ and choose a basis by enumerating elements of the Galois group. We denote this basis

$$\{\psi_1, ..., \psi_{n_L}\}.$$

We define an inner product on $\mathbb{Z}[\mathrm{Gal}(L/\mathbb{Q})]$ by letting

$$\langle \psi_i, \psi_j \rangle = \begin{cases} 1 & \text{if } i = j \\ 0 & \text{if } i \neq j, \end{cases}$$

and extending $\mathbb{Z}$-bilinearly.

Consider one of the T_i. For a fixed embedding

$$\xi : X^*(T_i) \hookrightarrow X^*(R_L),$$

and a chosen basis

$$\{\chi_1, ..., \chi_{d_i}\},$$

where d_i will denote the dimension of T_i, let m_ξ denote

$$\max\{|\langle \chi_j, \psi_k \rangle|\} \in \mathbb{N},$$

for $j = 1, ..., d_i$ and $k = 1, ..., n_L$. For each T_i we choose an embedding of $X^*(T_i)$ into $X^*(R_L)$ and a basis such that m_ξ is minimal i.e. the coordinates of this basis, with respect to the canonical basis of $X^*(R_L)$, have the smallest upper bound amongst all possible choices.

Thus, we have a collection of surjective maps of tori

$$R_L \to T_i.$$

We consider their direct product, yielding another surjection

$$R_L^s \to T_1 \times \cdots \times T_s.$$

Now, since T is isogenous to $T_1 \times \cdots \times T_s$, we may choose a surjection

$$\lambda : T_1 \times \cdots \times T_s \to T,$$

with kernel of smallest degree, which we will denote by n_λ.

We denote the composition of our product map with λ as

$$r : R_L^s \to T,$$

another surjective morphism.

Lemma 4.2 *Consider the morphism*

$$f : R_L^s \to T_1 \times \cdots \times T_s,$$

the direct product of the previously defined surjections of R on to the T_i, each followed by raising to the power n_λ. Then there exists a unique morphism,

$$g : T \to T_1 \times \cdots \times T_s,$$

such that $f = g \circ r$.

Proof. Let S be the kernel of r. By the universal property of quotients, any morphism from R_L^s vanishing on S factors uniquely through r. □

5 Uniform boundedness.

Firstly, we recall a standard property of integral matrix groups due to Minkowski.

Theorem 5.1 *For any $d \in \mathbb{N}$, the number of isomorphism classes of finite groups contained in $GL_d(\mathbb{Z})$ is finite.*

We have fixed an algebraic torus T over $\mathbb{Q}$ of dimension d with splitting field L. In other words, for any choice of basis, we have a faithful representation

$$\rho : Gal(L/\mathbb{Q}) \hookrightarrow GL_d(\mathbb{Z}).$$

Thus, by the previous theorem, $n_L = |Gal(L/\mathbb{Q})|$ is bounded in terms of the dimension of T only.

Secondly, we refer to a standard result from the theory of integral representations of finite groups [6].

Theorem 5.2 *Let H be a finite group and let $d \in \mathbb{N}$. Then the number of isomorphism classes of integral representations of H of dimension d is finite.*

Recall, then, that we chose a surjection

$$\lambda : T_1 \times \cdots \times T_s \to T,$$

with kernel of smallest degree n_λ. Tori over $\mathbb{Q}$ with splitting field L induce d-dimensional representations of the Galois group of L. By Theorem 5.1, there are only finitely many choices for this group. Therefore, by Theorem 5.2, only finitely many isomorphism classes of such tori exist. Therefore, n_λ is bounded in terms of d only.

Recall, also, that we constructed

$$f : R_L^s \to T_1 \times \cdots \times T_s,$$

via the composition of our original direct product of surjections and raising to the power n_λ. This corresponds to embeddings

$$X^*(T_i) \hookrightarrow X^*(R_L),$$

for each i. We have chosen the canonical basis for $X^*(R_L)$ and we choose the bases for the $X^*(T_i)$ to be the bases chosen in the previous section, all multiplied by n_λ. The previously stated results yield the following:

Lemma 5.3 *The coordinates of these bases for the $X^*(T_i)$ with respect to the canonical basis of $X^*(R_L)$ are bounded in terms of d only.*

6 Uniformisers.

We have identified $X^*(R_L)$ with $\mathbb{Z}[\mathrm{Gal}(L/\mathbb{Q})]$ and chosen the canonical basis $\{\psi_1, ..., \psi_{n_L}\}$ by enumerating the elements of the Galois group. The inner product on $X^*(R_L)$ satisfies the invariance property

$$\langle \sigma\psi, \psi' \rangle = \langle \psi, \sigma^{-1}\psi' \rangle,$$

for any $\sigma \in \mathrm{Gal}(L/\mathbb{Q})$ and $\psi, \psi' \in X^*(R_L)$. Now, $X^*(R_L)$ is naturally isomorphic to its dual $\mathbb{Z}[\mathrm{Gal}(L/\mathbb{Q})]$-module $\mathrm{Hom}(X^*(R_L), \mathbb{Z})$, sending ψ_i to $\langle \psi_i, - \rangle$, which we denote φ_i, and extending $\mathbb{Z}$-linearly. Via our perfect pairing

$$X_*(R_L) \times X^*(R_L) \to \mathbb{Z},$$

we have an isomorphism of $X_*(R_L)$ with the dual of $X^*(R_L)$. We identify φ_i with its image in $X_*(R_L)$. Thus, we obtain a basis

$$\{\varphi_1, ..., \varphi_{n_L}\}$$

of $X_*(R_L)$, which is that obtained by enumerating the elements of $\mathrm{Gal}(L/\mathbb{Q})$.

Let p be a rational prime, completely split in L. The basis

$$\{\chi_1, ..., \chi_{n_L}\}$$

induces an isomorphism of $R_L(\mathbb{Q}_p)$ with

$$\prod \mathbb{Q}_p^* \approx X_*(R_L) \otimes \mathbb{Q}_p^*.$$

Let P be the element of $R_L(\mathbb{Q}_p)$ such that $\chi_1(P) = p$ and $\chi_i(P) = 1$ for $i = 2, ..., n_L$. In fact, P is a uniformiser corresponding to a place lying above p and the Galois orbit of its image under the above isomorphism corresponds to a complete set of uniformisers at places lying above p.

We have a morphism from $X_*(R_L) \otimes \mathbb{Q}_p^*$ to $X_*(R_L)$, applying the valuation map

$$\upsilon_p : \mathbb{Q}_p^* \to \mathbb{Z}$$

to each factor. Under this morphism, P is sent to the basis element φ_1 and the Galois orbit of P yields the complete set of basis elements.

Now let l be a natural number and let $p_1, ..., p_l$ be rational primes completely split in L. For each p_i, let P_i be the element of $R_L(\mathbb{Q}_{p_i})$ associated to p_i via the above construction. We embed each $R_L(\mathbb{Q}_{p_i})$ into

$$R_L(\mathbb{A}_f) = (\mathbb{A}_f \otimes L)^*$$

in the natural way. For integers $a_1, ..., a_l$, we consider the element

$$I = P_1^{a_1} \cdots P_l^{a_l}$$

belonging to $R_L(\mathbb{A}_f)$.

Recall that we have a surjective map of $\mathbb{Q}$-tori,

$$r : R_L^s \to T.$$

Following [7], we have an induced map on the corresponding class groups, which we denote

$$r_h : h_{R_L^s} \to h_T.$$

Let $H = h_{R_L^s}/\ker r_h$. We will show that

$$\mathcal{M}_H(l) > \frac{c \log \Delta_L}{\log(l) + \log\log \Delta_L},$$

for any $l \in \mathbb{N}$, provided Δ_L is greater than a uniform constant. Since H injects into h_T, it is an easy observation that $\mathcal{M}_{h_T}(l) \geq \mathcal{M}_H(l)$, for $l \in \mathbb{N}$, thus yielding (1).

Henceforth, let I_i denote the embedding of I into the i^{th} factor of $R_L^s(\mathbb{A}_f)$. We denote by $\underline{I}$ the product of the I_i i.e. I embedded diagonally into $R_L^s(\mathbb{A}_f)$. Recall that, by Lemma 4.2, we have the following commutative diagram.

$$\begin{array}{ccccc} R_L^s(\mathbb{A}_f) & \rightarrow & T_1(\mathbb{A}_f) \times \cdots \times T_s(\mathbb{A}_f) & \rightarrow & T(\mathbb{A}_f) \\ & \searrow^{f} & & \swarrow^{g} & \\ & & T_1(\mathbb{A}_f) \times \cdots \times T_s(\mathbb{A}_f) & & \end{array}$$

with r being the composite homomorphism from $R_L^s(\mathbb{A}_f)$ to $T(\mathbb{A}_f)$.

Assume that $\underline{I}$ belongs to the kernel of r_h i.e.

$$r(\underline{I}) = \pi k \in T(\mathbb{Q})K_T^m,$$

where this product is unique up to an element of $T(\mathbb{Q}) \cap K_T^m$, which, by Theorem 2.5 of [10], is a finite group of order bounded in terms of the dimension of T only. Now, $f(\underline{I}) = g(\pi k)$, but f is a product of morphisms from $R_L(\mathbb{A}_f)$ into the $T_i(\mathbb{A}_f)$, so we write $f(\underline{I})$ as

$$(f_1(I), ..., f_s(I)).$$

As g is a morphism into $T_1(\mathbb{A}_f) \times \cdots \times T_s(\mathbb{A}_f)$, we write $g(\pi k)$ as

$$(g_1(\pi k), ..., g_s(\pi k)).$$

Thus, we have

$$f_i(I) = \pi_i k_i \in T_i(\mathbb{Q}) K^m_{T_i},$$

for $i = 1, ..., s$, where $\pi_i = g_i(\pi)$ and $k_i = g_i(k)$.

Now, recall the bases for the $X^*(T_i)$ under the embeddings into $X^*(R_L)$ induced by the f_i. We denote their elements as $\chi_{i,j}$, where $i = 1, ..., s$ and $j = 1, ..., d_i$. Furthermore, let

$$\pi_{i,j} = \chi_{i,j}(\pi_i).$$

The following lemma is a generalisation of Lemma 2.13 of [10] to the case of a torus covered by an arbitrary finite product of quasisplit tori.

Lemma 6.1 *The field L' generated over $\mathbb{Q}$ by the $\pi_{i,j}$ is L.*

Proof. Clearly $L' \subseteq L$, so let $\sigma \in \mathrm{Gal}(L/\mathbb{Q})$ and assume that σ acts trivially on L'. We need to show that such a σ is itself trivial. We have a faithful representation of $\mathrm{Gal}(L/\mathbb{Q})$ on the product of the $X_*(T_i)$ and, thus, it is equivalent to show that σ acts trivially on each $X_*(T_i) \otimes \mathbb{Q}$.

Recall our surjective maps of tori from R_L to T_i, which we denoted f_i. After tensoring our cocharacter modules with $\mathbb{Q}$ we retrieve short exact sequences

$$0 \to \mathbb{Q} \otimes \Delta_i \to \mathbb{Q} \otimes \Gamma \to \mathbb{Q} \otimes X_*(T_i) \to 0,$$

where $\Gamma = \mathbb{Z}[\mathrm{Gal}(L/\mathbb{Q})]$ and the Δ_i are Γ-submodules of $X_*(R_L) \cong \Gamma$. They correspond to the kernels of our surjections, which we denote N_i. We will show that σ acts trivially on the

$$\mathbb{Q} \otimes (X_*(R_L)/X_*(N_i)).$$

We will consider in turn the elements I_i. Since f is a product of the maps f_i, we will consider the I_i as belonging to $R_L(\mathbb{A}_f)$ mapping into $T_i(\mathbb{A}_f)$. The elements under scrutiny here are the $\pi_i \in T_i(\mathbb{Q})$, which are diagonally embedded in $T_i(\mathbb{A}_f)$. Therefore, we relabel p_1, P_1 and a_1 as p, P and a, respectively, and project from $R_L(\mathbb{A}_f)$ to $R_L(\mathbb{Q}_p)$ i.e. we turn our attention from I_i to its image $P^a \in R(\mathbb{Q}_p)$, mapping under f_i to $\pi_i k_{i,p}$, where $k_{i,p}$ is the p-component of k_i.

Since p splits each T_i, we also have isomorphisms

$$T_i(\mathbb{Q}_p) \approx X_*(T_i) \otimes \mathbb{Q}_p^*,$$

sending $x \in T_i(\mathbb{Q}_p)$ to

$$(\chi_{i,1}(x), ..., \chi_{i,d_i}(x)),$$

where we tacitly assume a choice

$$\{\mu_{i,1}, ..., \mu_{i,d_i}\}$$

of the natural dual basis to our character basis already chosen; as described earlier for R_L. The valuation $\upsilon_p : \mathbb{Q}_p^* \to \mathbb{Z}$ evaluates each factor, inducing an isomorphism between $T_i(\mathbb{Q}_p)/K^m_{T_i,p}$ and $X_*(T_i)$, where $K^m_{T_i,p}$ is the maximal compact open subgroup of $T_i(\mathbb{Q}_p)$.

We have the following commutative diagrams

$$\begin{array}{ccc} R_L(\mathbb{Q}_p) & \longrightarrow & X_*(R_L) \\ \downarrow & & \downarrow \\ T_i(\mathbb{Q}_p)/K^m_{T_i,p} & \longrightarrow & X_*(T_i), \end{array}$$

where the bottom arrow is the isomorphism just mentioned and the top arrow is the corresponding quotient version for $R_L(\mathbb{Q}_p)$ described earlier. The righthand arrow is the map of cocharacters induced by f_i and the left arrow is f_i composed with factoring out by $K^m_{T,p}$.

The element P^a is mapped to the class of π_i in $T_i(\mathbb{Q}_p)/K^m_{T_i,p}$, which is mapped to

$$(\upsilon_p(\chi_{i,1}(\pi_i)), ..., \upsilon_p(\chi_{i,d_i}(\pi_i))) \in X_*(T_i).$$

On the other hand, P^a is mapped to

$$(\upsilon_p(\psi_1(P^a)), ..., \upsilon_p(\psi_{n_L}(P^a))) \in X_*(R_L),$$

which is $a\varphi_1$. In this form, the action of a $\tau \in \mathrm{Gal}(L/\mathbb{Q})$ is clear, sending this image to

$$(\upsilon_p((\tau^{-1}\psi_1)(P^a)), ..., \upsilon_p((\tau^{-1}\psi_{n_L})(P^a))).$$

Note that, since $\mathrm{Gal}(L/\mathbb{Q})$ permutes the characters, the Galois orbit of the image of P^a comprises precisely the elements $a\varphi_i$, which consititute a basis for $X_*(R_L) \otimes \mathbb{Q}$.

We claim that the image of this orbit in $X_*(T_i)$ consists of the elements

$$(\upsilon_p((\tau^{-1}\chi_{i,1})(\pi_i)), ..., \upsilon_p((\tau^{-1}\chi_{i,d_i})(\pi_i))) \in X_*(T_i). \qquad (2)$$

To see this, let $\tau\mu_{i,j}$ be denoted by

$$\sum_{k=1}^{d_i} n_{j,k}^{i,\tau}\mu_{i,k}.$$

Thus, the image of

$$\sum_{j=1}^{d_i} \chi_{i,j}(\pi_i)\mu_{i,j} \in X_*(T_i) \otimes \mathbb{Q}_p^*$$

under $\tau \in \mathrm{Gal}(L/\mathbb{Q})$ will be

$$\sum_{k=1}^{d_i}\sum_{j=1}^{d_i} n_{j,k}^{i,\tau}\chi_{i,j}(\pi_i)\mu_{i,k}.$$

The k^{th} coefficient here is equal to $(\tau^{-1}\chi_{i,k})(\pi_i)$ if we have $n_{k,j}^{i,\tau^{-1}} = n_{j,k}^{i,\tau}$, for all $j, k = 1, ..., d_i$, but this is simply the Galois invariance of the inner product we previously placed on $X^*(R_L)$.

Now, since σ fixes each $\pi_{i,j}$ and the characters $\chi_{i,j}$ are the basis of a $\mathbb{Z}[\mathrm{Gal}(L/\mathbb{Q})]$-module, σ clearly fixes each of the elements of $X_*(T_i)$ depicted in (2). Thus, by our exact sequence, σ fixes the Galois orbit of the image of P^a in

$$\mathbb{Q} \otimes (X_*(R_L)/X_*(S_i)).$$

Since these elements span the above space, the claim follows.

□

Remark 6.2 *It is worth noting that any element in $R_L^s(\mathbb{A}_f)$ with a nonzero valuation at a place lying above a split prime in each of the s factors produces generators for L via this argument.*

7 Small split primes.

The remainder of the proof follows the concluding pages of [7].

We have $I = P_1^{a_1} \cdots P_l^{a_l} \in R_L(\mathbb{A}_f)$ embedded diagonally into $R_L^s(\mathbb{A}_f)$. We denote this element $\underline{I}$. The image of $\underline{I}$ in $T_1(\mathbb{A}_f) \times \cdots \times T_l(\mathbb{A}_f)$ under f is

$$f(\underline{I}) = (\pi_1 k_1, ..., \pi_l k_k) \in T_1(\mathbb{Q})K_{T_1}^m \times \cdots \times T_l(\mathbb{Q})K_{T_l}^m.$$

We consider the images $\pi_{i,j}$ of the π_i under the elements $\chi_{i,j}$ of the character bases. Due to Lemma 5.3, we have a bound B, say, on the coordinates of these basis elements with respect to the canonical basis of $X^*(R_L)$. This bound is dependent on d only. We replace the $\pi_{i,j}$ by $(p_1^{|a_1|} \cdots p_l^{|a_l|})^B \pi_{i,j}$, which belong to $\mathcal{O}_L$, the ring of integers of L.

By virtue of Lemma 6.1, we may form a primitive element

$$\alpha = \sum_{i,j} a_{i,j} \pi_{i,j}$$

for the field L, where the $a_{i,j}$ are integers with absolute value bounded by some constant E depending only on d. We take the $\mathbb{Q}$-basis $\{1, \alpha, \alpha^2, ..., \alpha^{n_L - 1}\}$ for L. Consequently, $\mathbb{Z}[1, \alpha, \alpha^2, ..., \alpha^{n_L-1}]$ is an order in $\mathcal{O}_L$. We denote the absolute value of its discriminant as Δ'_L. Therefore,

$$\Delta'_L \geq \Delta_L.$$

On the other hand, Δ'_L is the square of the determinant of the matrix

$$(\tau_i(\alpha^j))_{i,j},$$

where the τ_i range over the elements of $\mathrm{Gal}(L/\mathbb{Q})$ and $0 \leq j \leq n_L - 1$. An inequality of Hadamard then states that, given an upper bound C on the the values of

$$|\tau_i(\alpha^j)|,$$

then

$$\Delta'_L \leq n_L^{n_L} C^{2n_L} \leq c_1 C^{n_L},$$

where $c_1 > 0$ is a constant bounded in terms of d only.

The splitting field L of T is a Galois CM-field. For a character χ, we denote by $\overline{\chi}$ the image of χ under the automorphism of L induced by complex conjugation on $\mathbb{C}$. It is at this point that we use the fact that $T(\mathbb{R})$ is compact and is, therefore, a product of circles (see [8], Section 10.1). This implies that $\chi_{i,j}\overline{\chi_{i,j}}$ is the trivial character for every i and j (writing the group law multiplicatively).

Thus, for each $\tau \in \mathrm{Gal}(L/\mathbb{Q})$,

$$|\tau(\pi_{i,j})| = (p_1^{|a_1|} \cdots p_l^{|a_l|})^B$$

and, therefore, by the preceeding discussion,

$$|\tau_i(\alpha^j)| \leq (dE(p_1^{|a_1|} \cdots p_l^{|a_l|}))^{B(n_L-1)}.$$

Hence, our calculation yields

$$c_1^{-1}\Delta_L \leq (dE(p_1^{|a_1|} \cdots p_l^{|a_l|}))^{2Bn_L(n_L-1)}.$$

It remains to find the p_i for any given l. We require the following corollary of a special case of the effective Chebotarev Density Theorem, a proof of which can be found in [1].

Theorem 7.1 *Let F be any number field. Assume the Generalised Riemann Hypothesis holds for the Dedekind zeta function of F. Let $\pi_F(x)$ denote the number of rational primes p completely split in F such that $p \leq x$. There exist positive, absolute constants c_2 and c_3 that are effectively calculable such that, for all $x \geq c_2(\log \Delta_F)^2(\log\log \Delta_F)^4$,*

$$\pi_F(x) \geq c_3 \frac{x}{\log x}.$$

We assume the Generalised Riemann Hypothesis for CM fields. Let l be any natural number. We require at least l primes completely split in L, so let

$$x = c_4 l \log l + c_1(\log \Delta_L)^2(\log\log \Delta_L)^4 > 1,$$

where c_4 is a positive, absolute constant, such that

$$c_3 \frac{x}{\log x} \geq l.$$

It is uniform since

$$\frac{x}{\log x} \geq \frac{c_4 l \log l}{\log c_4 + 2\log l},$$

and so our requirement is satisfied when, for example, $\frac{c_3 c_4}{\log c_4 + 2} \geq 1$.

Thus, by Theorem 7.1, we are able to find l primes $p_1, ..., p_l$ completely split in l such that $p_i \leq x$. Subsequently, we return to our inequality

$$c_1^{-1}\Delta_L \leq (dE(p_1^{|a_1|} \cdots p_l^{|a_l|}))^{2Bn_L(n_L-1)},$$

choosing for the p_i those just found. As before, we let

$$A = \sum_{i=1}^{l} |a_i|,$$

yielding

$$\log(F^{-1}\Delta_L) \leq 2ABn_L(n_L - 1)\log x,$$

provided $\Delta_L > F$, where $F = c_1(dE)^{2Bn_L(n_L-1)}$. Now, there exists a positive, absolute constant c_5 such that

$$\log x \leq c_5(\log l + \log\log\Delta_L),$$

provided Δ_L exceeds a positive, absolute constant. Combining these two inequalities yields a lower bound for A, which implies (1).

□

Remark 7.2 *The constant c given in the statement of (1) will be* $\frac{c_6}{2Bn_L(n_L-1)}$*, where* c_6 *can be taken to be* $1-\epsilon$*, for any* $0 < \epsilon < 1$*, with each value of* ϵ *setting a uniform lower bound on the size of* Δ_L*.*

Bibliography.

[1] Amoroso, F and Dvornicich, R (2003), *Lower Bounds for the Height and Size of the Ideal Class Group in CM-Fields*, Monatsh. Math. 138, 85-94

[2] Daileda, R. C., Krishnamoorthy, R and Malyshev, A (2009), *Maximal Class Numbers of CM Number Fields*, Preprint.

[3] Ellenberg, J.S. and Venkatesh, A (2007), *Reflection principles and bounds for class group torsion*, Internat. Math. Res. Not. doi: 10.1093/imrn/rnm002

[4] Platanov, V. P. and Rapinchuk, A. S. (1991), *Algebraic Groups and Number Theory*, Academic Press, Inc.

[5] Suprunenko, D. A. and Hirsch K. A. (1999), *Matrix Groups*, American Mathematical Soc.

[6] Tsimerman, J (2011), *Brauer-Siegel theorem for tori*, Preprint.

[7] Ullmo, E and Yafaev, A (2011), *Nombre de classes des tores de multiplication complexe et bornes inférieures pour orbites Galoisiennes de points spéciaux*, Preprint.

[8] Voskresensky, V.E. (1998) *Algebraic groups and their birational invariants*, American Mathematical Soc.

[9] Waterhouse, W.C. (1979), *Introduction to Affine Group Schemes*, Springer-Verlag New York Inc.

[10] Yafaev, A (2006), *A conjecture of Yves André*, Duke Math. J. 132, no. 3, 393-407

[11] Zhang, S-W (2005), *Equidistribution of CM-Points on Quaternion Shimura Varieties*, Int. Math. Res. Not., no. 59, 3657-3689