Radicals in arithmetic

Palenstijn, W.J.

Author: Palenstijn, Willem Jan
Title: Radicals in Arithmetic
Issue Date: 2014-05-22

Chapter 6

Artin's primitive root conjecture for rank one tori

6.1 Introduction

The theory we set up in Chapter 2 is applicable in a wider setting than that of radicals over fields which we have studied so far. In this chapter, we use it for *division points* of rank one tori. After briefly introducing the concept of a torus, we state analogues of Artin's primitive root density question and a conjectured density theorem for rank one tori over number fields. For tori defined over $\mathbf{Q}$, these densities have previously been computed by Chen [7].

An *algebraic group* is an algebraic variety with a group operation. A well-known example is the algebraic group called $\mathbf{G}_{\mathrm{m}}$, defined as an affine variety by the equation

$$xy = 1$$

and the group law

$$(x, y)(x', y') = (xx', yy').$$

For any commutative ring R, the map $(x, y) \mapsto x$ gives an isomorphism of the group $\mathbf{G}_{\mathrm{m}}(R)$ to the unit group R^* of R.

Definition 6.1. A *torus* over a field K is an algebraic group that is isomorphic to $\mathbf{G}_{\mathrm{m}}^r$ over K^{sep} for some positive integer r. This integer r is called the *rank* of the torus.

If an algebraic group G over K is isomorphic to $\mathbf{G}_{\mathrm{m}}^r$ for $r \in \mathbf{Z}_{>0}$ over a field $L \supset K$, then we say G is *split* over L.

If T is a torus of rank r defined over a number field K, the group of *division points* of such a torus is given by

$$\{P \in T(K^{\mathrm{sep}}) : \exists n \in \mathbf{Z}_{>0} : P^n \in T(K)\}.$$

The torsion subgroup of this group is isomorphic to $(\mathbf{Q}/\mathbf{Z})^r$. To satisfy our condition on radical group extensions that all finite subgroups are cyclic, we therefore restrict to tori of rank 1. If K has characteristic 0, the group of division points is then isomorphic to the maximal radical extension of $T(K)$ as defined by Theorem 2.1. For characteristic $p > 0$ this holds if we make the adjustments mentioned in Remark 2.11.

We shall later show that all tori of rank one over a field K can be described as follows. If $f = X^2 + aX + b$ is a separable monic quadratic polynomial over K, let α be the zero X of f in the quadratic K-algebra $L = K[X]/(f)$.

We can then define an algebraic group T with equation and group law given by

$$x^2 + axy + by^2 = 1;$$

$$(x, y)(x', y') = (xx' - yy'b, xy' + x'y + yy'a).$$

The map sending a point $(x, y) \in T(K)$ to $(x - y\alpha) \in L$ gives a group isomorphism between $T(K)$ and the kernel of the norm map $N_K^L : L^* \to K^*$. In particular, if f factors as a product of two linear polynomials, then T is isomorphic to $\mathbf{G}_\mathrm{m}$ over K. If on the other hand f is irreducible, then T is split over the quadratic extension field L defined by f.

From here on, let T be the rank one torus defined over a number field K by the quadratic polynomial f.

Define S to be the set of primes of K that occur in the denominators of the coefficients of f or in the discriminant of f. Then we say that T has *good reduction* at all primes outside of S, in the following sense. For a prime $\mathfrak{q} \notin S$, the torus T is defined over the local ring $\mathcal{O}_{K,\mathfrak{q}}$, given by

$$\mathcal{O}_{K,\mathfrak{q}} = \{x \in K : \mathrm{ord}_\mathfrak{q}(x) \geq 0\}.$$

There is then a reduction map which gives a group homomorphism:

$$T(\mathcal{O}_{K,\mathfrak{q}}) \to T(\mathcal{O}_K/\mathfrak{q}).$$

Since $\mathfrak{q}$ does not divide the discriminant of f, the equation f taken modulo $\mathfrak{q}$ defines a torus $\bar{T}$ over $\mathcal{O}_K/\mathfrak{q}$. The group $T(\mathcal{O}_K/\mathfrak{q}) = \bar{T}(\mathcal{O}_K/\mathfrak{q})$ is then a subgroup of the unit group of its (finite) splitting field, and is therefore cyclic.

Also, for a point P of $T(K)$, we have that for almost all primes $\mathfrak{q}$ the point P is in $T(\mathcal{O}_{K,\mathfrak{q}})$ and the reduction $\bar{P} \in T(\mathcal{O}_K/\mathfrak{q})$ is well-defined. Because of these properties, there is an analogue of Artin's primitive root density question for rank one tori.

Question 6.2. *If P is a point of $T(K)$, for how many primes $\mathfrak{q}$ of $\mathcal{O}_K$ is the group $T(\mathcal{O}_K/\mathfrak{q})$ generated by $\bar{P}$?*

If T is $\mathbf{G}_\mathrm{m}$ and $K = \mathbf{Q}$, this is exactly the original question Artin asked. In this chapter we will work in greater generality, analogously to Chapter 5. With K a number field and T a rank one torus defined over K, let V be a finitely generated subgroup of $T(K)$ that is not contained in $T(K)_\mathrm{tors}$, and let t be a positive integer.

We will look at the set $M = M(T, V, t)$ of primes $\mathfrak{q}$ of K satisfying:

- $v \in T(\mathcal{O}_{K,\mathfrak{q}})$ for all $v \in V$; and
- $[T(\mathcal{O}_K/\mathfrak{q}) : \bar{V}] \mid k$.

We again reduce this to an expression about automorphism groups of radical group extensions and their entanglement. Choose a fixed algebraic closure $\bar{K}$ of K. As in the previous chapter, for a rational prime p, let $e(p)$ be the smallest positive integer such that $p^{e(p)}$ does not divide t, and define the radical group extensions

$$T(K) \subset B_p = \big\langle T(K), \{z \in T(\bar{K}) : z^{p^{e(p)}} \in V\}\big\rangle.$$

We also define $A_p = \mathrm{Aut}_{T(K)}(B_p)$, and B as the subgroup of $T(\bar{K})$ generated by all B_p. The absolute Galois group G_K of K acts on $T(\bar{K})$ as described above, and this action induces a map G_K to $A = \mathrm{Aut}_{T(K)}(B)$ with as cokernel the abelian entanglement group $E = E(B)$.

In the present setting, we get the same two main theorems as in Chapter 5.

Theorem 6.3. *The entanglement group $E(B)$ of B is finite.*

Theorem 6.4. *Assuming GRH, the set $M(T, V, t)$ has a natural density equal to*

$$C(T, V, t) \cdot \prod_{p \text{ prime}} \left(1 - \frac{1}{\#A_p}\right),$$

where $C(T, V, t)$ is a rational correction factor given by

$$C(T, V, t) = \sum_{\chi \in E^\vee} \prod_{\substack{p \text{ prime} \\ \chi(A_p) \neq 1}} \frac{-1}{\#A_p - 1}.$$

We prove these results in Section 6.3. In the remainder of the chapter, we give results to make the necessary computations explicit, and illustrate this with a number of examples in Section 6.4.

6.2 Preliminaries

Let K be a field. One can show (see e.g., Borel [5], §8) that there is a covariant equivalence of categories

$$\{\text{rank } r \text{ tori over } K\}$$
$$\longleftrightarrow$$
$$\{\text{rank } r \text{ free abelian groups with continuous } \mathrm{Gal}(K^{\mathrm{sep}}/K)\text{-action}\}.$$

Following the notation from [5], this maps a torus T to $X_*(T) = \mathrm{Mor}(\mathbf{G}_\mathrm{m}, T)$.

We also have the following Galois module isomorphism.

$$\begin{array}{rcl} \bar{K}^* \otimes_{\mathbf{Z}} X_*(T) & \xrightarrow{\sim} & T(\bar{K}) \\ z \otimes f & \longmapsto & f(z). \end{array}$$

Here the Galois group acts on both factors on the left separately. In particular, a rank one torus T over K corresponds to the infinite cyclic group with an action of $\mathrm{Gal}(K^{\mathrm{sep}}/K)$, and we choose a fixed generator τ. If the Galois action on τ is trivial, then T is isomorphic to the torus $\mathbf{G}_{\mathrm{m}}$ over K.

If the action is not trivial, then there is a field L of degree 2 over K such that the action factors via the quotient $\mathrm{Gal}(L/K)$ of $\mathrm{Gal}(K^{\mathrm{sep}}/K)$ because $\mathrm{Aut}(\mathbf{Z})$ equals $\{\pm 1\}$. In this case, T is not split over K, but it is split over L, and more generally over all fields containing L. Let σ be an element of $\mathrm{Gal}(K^{\mathrm{sep}}/K)$. The Galois action on τ is then explicitly given by

$$\sigma(\tau) = \begin{cases} \tau & \text{if } \sigma|_L = \mathrm{id}; \text{ and} \\ -\tau & \text{if } \sigma|_L \neq \mathrm{id}. \end{cases}$$

We can use the morphism $\tau \in \mathrm{Mor}(\mathbf{G}_{\mathrm{m}}, T)$ to twist the Galois action on $\bar{K}^*$. If z is an element of $\bar{K}^*$, then, using the Galois module isomorphism above, $z \otimes \tau$ gives a point on the torus. Since $\bar{K}^*$ is a multiplicatively written module, we write $z^\tau = z \otimes \tau$. Because τ is a generator of $X_*(T) = \mathrm{Mor}(\mathbf{G}_{\mathrm{m}}, T)$, we then also have $\bar{K}^{*\tau} = \bar{K}^* \otimes_{\mathbf{Z}} X_*(T)$, with an induced isomorphism of Galois modules:

$$\begin{array}{rcl} \bar{K}^{*\tau} & \xrightarrow{\sim} & T(\bar{K}) \\ z^\tau & \longmapsto & \tau(z) \end{array}$$

In this chapter, we will view this as an identification, and consider z^τ as a point of $T(\bar{K})$. This notation allows us to conveniently write the action of $\mathrm{Gal}(K^{\mathrm{sep}}/K)$ on $T(\bar{K})$ as

$$\sigma(z^\tau) = \sigma(z)^{\sigma(\tau)},$$

where $\sigma(z)$ is the usual Galois action on $\bar{K}$.

Note that the map $z \mapsto z^\tau$ gives a bijection of $\bar{K}^* \to T(\bar{K})$, but this does not respect the Galois action of $\mathrm{Gal}(K^{\mathrm{sep}}/K)$.

In characteristic 0, each non-split rank one torus over K is isomorphic to a torus T_d defined by the norm equation of $K(\sqrt{d})/K$,

$$T_d : x^2 - dy^2 = 1,$$

with multiplication of two points (x, y) and (x', y') defined by

$$(x, y)(x', y') = (xx' + dyy', xy' + x'y).$$

For one of the two choices of generator $\tau \in X_*(T)$, the Galois module isomorphism with $\bar{K}^{*\tau}$ is then given as

$$\begin{array}{rcl} T_d(\bar{K}) & \xrightarrow{\sim} & \bar{K}^{*\tau} \\ (x,y) & \longmapsto & (x - y\sqrt{d})^\tau. \end{array}$$

Sending (x, y) to $(x+y\sqrt{d})^\tau$ would correspond with the other choice of generator of $X_*(T)$.

Non-split rank one tori differ from the $\mathbf{G}_\mathrm{m}$ case in a number of interesting ways relevant to the topic of this thesis. For example, the torus T_{-1} defined by $x^2+y^2 = 1$ and splitting field $\mathbf{Q}(i)$ has rational 4-torsion. Similarly, the torus T_{-3} given by $x^2 + 3y^2 = 1$ has splitting field $\mathbf{Q}(\sqrt{-3}) = \mathbf{Q}(\zeta_3)$ and has rational 6-torsion. This means radical group extensions over these tori can have greater entanglement groups than similar examples over $\mathbf{G}_\mathrm{m}$, as we shall see in the examples in this chapter.

Another significant way in which they can differ from $\mathbf{G}_\mathrm{m}$ is that for negative d, the group of division points of $T_d(\mathbf{R})$ is divisible and contains non-trivial p-torsion for all primes p, so the maximal radical extension of $T_d(\mathbf{Q})$ in this case is contained in $T_d(\mathbf{R})$.

We conclude this section with remarks on notation. Let G_K be the absolute Galois group of K, and M a G_K-module. Then we can adjoin the Galois module M to K by defining $K(M)$ as the invariant field of the kernel of the action $G_K \to \mathrm{Aut}(M)$.

If M is a G_K-submodule of $\bar{K}^*$, then $K(M)$ is the field extension of K generated by M.

If M is a G_K-submodule of $T(\bar{K})$, or equivalently a Galois radical extension of $T(K)$ inside $T(\bar{K})$, then $K(M)$ is the field extension of K generated by the coordinates of the elements of M.

We have seen that if C is a Galois submodule of $\bar{K}^*$, then C^τ can be considered a Galois submodule of $T(\bar{K})$. For example, if μ is the group of all roots of unity of $\bar{K}^*$, then μ^τ is naturally isomorphic to $T(\bar{K})_\mathrm{tors}$ as a Galois module.

Note that the field extension $K(\mu^\tau)$ obtained by adjoining the Galois module μ^τ is in general not the same as the field extension $K(\mu)$ obtained by adjoining μ to K. Consider for example the torus T_{-1} defined by $x^2 + y^2 = 1$ over $\mathbf{Q}$, and μ the roots of unity of $\bar{\mathbf{Q}}^*$. Then the coordinates of μ^τ are real, and one can in fact show that for T_{-1} the field $\mathbf{Q}(\mu^\tau)$ is equal to $\mathbf{Q}(\mu) \cap \mathbf{R}$.

6.3 Proof of main theorems

In this section we will prove Theorems 6.3 and 6.4. The main ingredient for the correction factor being a rational number is that the entanglement group $E(B)$ of B as defined in Section 6.1 is finite.

We show this by proving the analogue of Theorem 5.5. As before, if n is a positive integer, we write B_n for the abelian group generated by all B_p for $p \mid n$.

Theorem 6.5. *Write w for the number of torsion points in $T(K)$ and let L be the splitting field of T. Define the integer n as the product of all primes p satisfying*

$$p \mid w\Delta_{L((B_w)_{\mathrm{ab}})/\mathbf{Q}}.$$

Then the natural map $E(B) \to E(B_n)$ is an isomorphism.

Proof. Before we start, note that if T is split over K, then this theorem reduces to Theorem 5.5, so we assume that T is not split over K.

We now mirror the proofs of Theorem 5.1 and Theorem 5.5. Specifically, define C_n and C'_n as follows.

$$\begin{aligned} C_n &= (B_n)_{\mathrm{ab}} \text{ and} \\ C'_n &= \left\langle T(K), \mu^{\tau}_{p^{e(p)}} : p \nmid n \right\rangle . \end{aligned}$$

By the same reasoning as for Theorem 5.1, we can decompose B_{ab} and $\mathrm{Aut}_{T(K)}(B_{\mathrm{ab}})$.

$$B_{\mathrm{ab}} = C_n \oplus_{T(K)} C'_n$$

$$\mathrm{Aut}_{T(K)}(B_{\mathrm{ab}}) = \mathrm{Aut}_{T(K)}(C_n) \times \mathrm{Aut}_{T(K)}(C'_n).$$

Apart from different notation, Equation 5.3 holds in this setting since its proof is purely group theoretic. Translated, it reads

$$p \nmid w \Rightarrow (B_p)_{\mathrm{ab}} = \mu^{\tau}_{p^{e(p)}} T(K).$$

Because $L(\mu^{\tau}_{p^{e(p)}})$ equals $L(\zeta_{p^{e(p)}})$, we can deduce from the previous statement that we have:

$$L(C_n) = L((B_n)_{\mathrm{ab}}) = L((B_w)_{\mathrm{ab}}, \zeta_{p^{e(p)}} : p \mid n) = L((B_w)_{\mathrm{ab}}) \cdot \mathbf{Q}(\zeta_{p^{e(p)}} : p \mid n).$$

Now following exactly the reasoning from the proof of Theorem 5.5, we arrive at the statement that $\mathrm{Gal}(L(B_{\mathrm{ab}})/L(C_n))$ maps surjectively to the Galois group $\mathrm{Gal}(\mathbf{Q}(\zeta_{p^{e(p)}} : p \nmid n)/\mathbf{Q})$, which is naturally isomorphic to $\mathrm{Aut}(\langle \mu_{p^{e(p)}} : p \nmid n\rangle)$.

Since $L(C_n)$ contains L, the action of the absolute Galois group $G_{L(C_n)}$ of $L(C_n)$ on $\mu^{\tau}_{p^{e(p)}}$ is the regular Galois action on $\mu_{p^{e(p)}}$, so the Galois action on the torus induces a surjection $G_{L(C_n)} \twoheadrightarrow \mathrm{Aut}_{T(K)}(C'_n)$.

Since the larger Galois group $G_{K(C_n)}$ also acts on $T(C'_n)$, we have a surjection $G_{K(C_n)} \twoheadrightarrow \mathrm{Aut}_{T(K)}(C'_n)$. This factors via $\mathrm{Gal}(K(B_{\mathrm{ab}})/K(C_n))$ since the absolute Galois group of $K(B_{\mathrm{ab}})$ acts as the identity on $C'_n \subset B_{\mathrm{ab}}$.

The proof now concludes exactly as the proof of Theorem 5.5. □

Proof of Theorem 6.4. Recall that for a rational prime p, we defined $e(p)$ to be the smallest positive integer such that $p^{e(p)}$ does not divide t.

Now let $\mathfrak{q}$ be a prime of K for which T has good reduction and for which V is contained in $\mathcal{O}_{K,q}$. These conditions only exclude a finite number of primes as we saw in the introduction, so this does not affect the density. For such a prime, $T(\mathcal{O}_K/\mathfrak{q})$ is well-defined and V can be mapped to $T(\mathcal{O}_K/\mathfrak{q})$.

The index $[T(\mathcal{O}_K/\mathfrak{q}) : \bar{V}]$ now divides t if and only if for all primes p, the index is not divisible by $p^{e(p)}$. Choose a rational prime p with $\mathfrak{q} \nmid p$, and write $e = e(p)$ for brevity.

We saw in the introduction that $T(\mathcal{O}_K/\mathfrak{q})$ is cyclic, so we find that

$$p^e \mid [T(\mathcal{O}_K/\mathfrak{q}) : \bar{V}]$$

if and only if

$$p^e \mid \#T(\mathcal{O}_K/\mathfrak{q}) \text{ and } \bar{V} \subset T(\mathcal{O}_K/\mathfrak{q})^{p^e}$$

if and only if

$$\#T(\mathcal{O}_K/\mathfrak{q}) \text{ has an element of order } p^e \text{ and } \bar{V} \subset T(\mathcal{O}_K/\mathfrak{q})^{p^e}.$$

This is in turn equivalent with

$$\mathfrak{q} \text{ splits completely in } K \subset K(\mu^\tau_{p^e}, \sqrt[p^e]{V}) = K_p.$$

If we write $G_n = \operatorname{Gal}(K_p/K)$ and $S_n = G_n \setminus \{1\}$, then our condition for $\mathfrak{q}$ at p is that the Frobenius of $\mathfrak{q}$ in K_p/K is in S_n.

This describes the condition for $\mathfrak{q}$ we have at the single prime p. To combine this for multiple primes, let n be a positive integer, and define the field K_n as the compositum of the fields K_p for $p \mid n$. Let G_n be $\operatorname{Gal}(K_n/K)$ and define S_n as

$$S_n = \{\sigma \in G_n : \sigma \mid_{K_p} \neq \text{id for all } p \mid n\}.$$

Assuming the Generalized Riemann Hypothesis, the work of Murty [25] provides the analytic number theory argument that the set of primes $\mathfrak{q}$ satisfying the condition at every prime has a density, and that the density is equal to the limit

$$\lim_{n \to \infty} \frac{\#S_n}{\#G_n}.$$

The derivation of the formula for the density we give in Theorem 6.4, including its correction factor as a character sum now proceeds entirely as in the proof of Theorem 5.2. □

6.4 Explicit density computations

In this section we show how to explicitly compute Artin densities, and in particular the entanglement groups involved.

Let T be a non-split rank one torus over a number field K, and let L be its splitting field, so L/K is a quadratic extension. Let $B \supset T(K)$ be a Galois radical group extension, and B_{ab} its maximal abelian subextension.

By using the strategy from Section 5.3 if necessary, we may assume that to compute Artin densities, we can take B_{ab} of the form $\mu^\tau W$, where μ^τ is a group of torsion division points of $T(\bar{K})$, and W is a set of Kummer roots of $T(\bar{K})$ with $T(K) \subset W$.

Corollary 2.29 (with $C = W$ and $D = \mu^\tau$) gives us an isomorphism

$$E(\mu^\tau W) \xrightarrow{\sim} \mathrm{Aut}_{\mu^\tau \cap W}(\mu^\tau)/\mathrm{im}(G_W).$$

Here G_W is the kernel of the action of the absolute Galois group G_K of K on W. We will come back to the exact map later, and start by considering the image of G_W in $\mathrm{Aut}(\mu^\tau)$. To aid in determining this, we start with a group theoretic technical proposition.

Proposition 6.6. *Let G be a group acting on an abelian group M via the map $\varphi : G \to \mathrm{Aut}(M)$. Let $\varepsilon : G \to \{\pm 1\}$ be a surjective group homomorphism, and define H to be the kernel of ε. Define the group homomorphism $\varepsilon\varphi$ as follows.*

$$\begin{array}{rcl} \varepsilon\varphi : G & \longrightarrow & \mathrm{Aut}(M) \\ g & \longmapsto & \varepsilon(g)\varphi(g) \end{array}$$

Then the following statements characterize $\varepsilon\varphi G$.

- *If $-1 \in \varphi H$, then $\varepsilon\varphi G = \varphi G$.*
- *If $-1 \in \varphi G \setminus \varphi H$, then $\varepsilon\varphi G = \varphi H$.*
- *If $-1 \notin \varphi G = \varphi H$, then $\varepsilon\varphi G = \langle \varphi G, -1\rangle$.*
- *If $-1 \notin \varphi G \neq \varphi H$, then $\varepsilon\varphi G$, and φG and $\langle \varphi H, -1\rangle$ are the three distinct index 2 subgroups of $\langle \varphi G, -1\rangle$ containing φH.*

$$\begin{tikzcd}
& \langle \varphi G, -1\rangle & \\
\langle \varphi H, -1\rangle \arrow[ur, hook] & \varphi G \arrow[u, hook] & \varepsilon\varphi G \arrow[ul, hook] \\
& \varphi H \arrow[ul, hook] \arrow[u, hook] \arrow[ur, hook] &
\end{tikzcd}$$

Proof. First of all, note that exactly one of the four statements applies to any given situation.

We write G as the disjoint union of H and $G \setminus H$, so $\varepsilon\varphi G = \varepsilon\varphi H \cup \varepsilon\varphi(G \setminus H)$. Because we have $\varepsilon H = 1$, we get $\varepsilon\varphi H = \varphi H$. We turn to $\varepsilon\varphi(G \setminus H)$.

Suppose that we have $-1 \in \varphi H$. Then there is an element $c \in H$ with $\varphi(c) = -1$. We see that $\varepsilon\varphi(G \setminus H) = \varphi c(G \setminus H) = \varphi(G \setminus H)$. In this case, we get $\varepsilon\varphi G = \varphi G$.

Next, suppose that $-1 \notin \varphi H$, but $-1 \in \varphi G$. Then there is an element $c \in (G \setminus H)$ with $\varphi(c) = -1$. We then have that $G \setminus H = cH$, so $\varepsilon\varphi(G \setminus H) = \varepsilon\varphi cH = -1 \cdot -1 \cdot \varphi H = \varphi H$. We get $\varepsilon\varphi G = \varphi H$.

For the final two statements, assume $-1 \notin \varphi G$, and pick an element $\sigma \in (G \setminus H)$. Then we get $\varepsilon\varphi(G \setminus H) = \varepsilon\varphi(\sigma H) = (-\varphi(\sigma))\varphi(H)$.

If we then additionally have $\varphi G = \varphi H$, then we continue with $(-\varphi(\sigma))\varphi(H) = -\varphi(\sigma)\varphi(G) = -\varphi(G)$, and we get $\varepsilon\varphi G = \varphi G \cup -\varphi G = \langle \varphi G, -1\rangle$.

Finally, if $-1 \notin \varphi G \neq \varphi H$, then φG and $\langle \varphi H, -1\rangle$ contain φH with index 2. Since $\varphi(\sigma)$ and -1 commute in M, they are both contained in $\langle \varphi G, -1\rangle$ with index 2, and there is a third distinct index 2 subgroup, which we claim is $\varepsilon\varphi G$, as shown in the diagram above.

To see this, note that $\varphi G = \varphi H \cup \varphi(\sigma)\varphi H$, and $\langle \varphi H, -1\rangle = \varphi H \cup -\varphi H$. The third subgroup is $\varphi H \cup -\varphi(\sigma)\varphi H$, which is exactly how we had rewritten $\varepsilon\varphi G$. $\square$

We use this proposition to determine the image of G_W in $\mathrm{Aut}(\mu^\tau)$ induced by the Galois action on μ^τ. To use the proposition in explicit examples, we first describe how we can apply it to the context of the torus T, taking $G = G_W$ acting on $M = \mu^\tau$.

Let $K(W)$ be the field obtained by adjoining the coordinates of the points in W to K. Then G_W is the absolute Galois group of $K(W)$. Recall that L is the splitting field of the torus T, so it is a quadratic field extension of K. Let H be the absolute Galois group of $L(W)$. It is a subgroup of index 2 of G_W. Let ε be the unique map $G_W \to \{\pm 1\}$ with kernel H.

We will now use Proposition 6.6 for the action of G_W on $\mu \subset \bar{K}$ compared to that of G_W on $\mu^\tau \subset T(\bar{K})$. The former is the regular Galois action, which we shall denote by $\varphi : G_W \to \mathrm{Aut}(\mu)$, while the latter is the Galois action on points of the torus, which is then given by $\varepsilon\varphi : G_W \to \mathrm{Aut}(\mu^\tau)$.

We now identify $\mathrm{Aut}(\mu)$ and $\mathrm{Aut}(\mu^\tau)$. Note that the induced diagram is *not* commutative:

$$\begin{tikzcd} G_W \arrow[r, "\varphi"] \arrow[dr, "\varepsilon\varphi"'] & \mathrm{Aut}(\mu) \arrow[d, "\mathrm{id}"] \\ & \mathrm{Aut}(\mu^\tau) \end{tikzcd}$$

We can then use Proposition 6.6 to explicitly obtain the Galois action $\varepsilon\varphi$ of G_W on $\mu^\tau = T(\bar{K})_{\mathrm{tors}}$ in terms of the regular Galois action φ on the roots of unity μ of $\bar{K}$.

In this situation, since $-1 \in \mathrm{Aut}(\mu)$ corresponds to complex conjugation in $\mathrm{Gal}(\mathbf{Q}^{\mathrm{ab}}/\mathbf{Q})$, the condition $-1 \in \varphi G$ is equivalent to $K(W) \cap \mathbf{Q}^{\mathrm{ab}} \subset \mathbf{R}$. The condition $-1 \in \varphi H$ is similarly equivalent to $L(W) \cap \mathbf{Q}^{\mathrm{ab}} \subset \mathbf{R}$. Also, the condition $\varphi G = \varphi H$ is equivalent to $K \cap \mathbf{Q}^{\mathrm{ab}} = L \cap \mathbf{Q}^{\mathrm{ab}}$.

Example 6.7.

As a first example, we will compute the entanglement group of the maximal cyclotomic extension of a torus. Specifically, let T be a rank one torus over a number field K with splitting field L, and let μ be the roots of unity in $\bar{K}$. Then μ^τ is naturally isomorphic as a Galois module to $T(\bar{K})_{\mathrm{tors}}$. We will determine $E(\mu^\tau)$ with the action of the absolute Galois group G_K of K.

In this example, we are only adjoining torsion points, so take $W = T(K)$. Using the terminology from above, we get $G_W = G_K$ and $H = G_L$.

Let w be the number of roots of unity in K. We take the expression for the entanglement group from the beginning of this section, and adapt it for the current example:

$$E(\mu^\tau) \xrightarrow{\sim} \mathrm{Aut}_{\mu^\tau \cap T(K)}(\mu^\tau)/\varphi(G_W).$$

If we identify $\mathrm{Aut}(\mu^\tau)$ with $\hat{\mathbf{Z}}^*$, the automorphism group $\mathrm{Aut}_{\mu^\tau \cap T(K)}(\mu^\tau)$ in this expression is identified with $(\hat{\mathbf{Z}}^* \cap (1 + w\hat{\mathbf{Z}}))$.

Next, write Γ_K for φG_K and Γ_L for φG_L. The proposition then leads to the following four cases.

If $L \cap \mathbf{Q}^{\mathrm{ab}}$ is real, then $\varepsilon\varphi G_K = \varphi G_K = \Gamma_K$, and we obtain

$$E(\mu^\tau) = \left(\hat{\mathbf{Z}}^* \cap (1 + w\hat{\mathbf{Z}})\right) \Big/ \Gamma_K.$$

If $L \cap \mathbf{Q}^{\mathrm{ab}}$ is not real, but $K \cap \mathbf{Q}^{\mathrm{ab}}$ is real, then $\varepsilon\varphi G_K = \varphi G_L = \Gamma_L$, and we get

$$E(\mu^\tau) = \left(\hat{\mathbf{Z}}^* \cap (1 + w\hat{\mathbf{Z}})\right) \Big/ \Gamma_L.$$

If $K \cap \mathbf{Q}^{\mathrm{ab}}$ is not real, and $K \cap \mathbf{Q}^{\mathrm{ab}} = L \cap \mathbf{Q}^{\mathrm{ab}}$, then $\varepsilon\varphi G_K = \langle \varphi G_K, -1\rangle$, and we obtain

$$E(\mu^\tau) = \left(\hat{\mathbf{Z}}^* \cap (1 + w\hat{\mathbf{Z}})\right) \Big/ \langle \Gamma_K, -1\rangle.$$

Finally, suppose $K \cap \mathbf{Q}^{\mathrm{ab}}$ is not real and $K \cap \mathbf{Q}^{\mathrm{ab}} \neq L \cap \mathbf{Q}^{\mathrm{ab}}$. Write $\mathbf{Q}^{\mathrm{ab}+}$ for $\mathbf{Q}^{\mathrm{ab}} \cap \mathbf{R}$. Then $\mathrm{Gal}(L \cap \mathbf{Q}^{\mathrm{ab}}/K \cap \mathbf{Q}^{\mathrm{ab}+})$ is isomorphic to V_4 as depicted in the diagram on the left below. The field M is the third distinct field between $K \cap \mathbf{Q}^{\mathrm{ab}+}$ and $L \cap \mathbf{Q}^{\mathrm{ab}}$. The figure on the right shows the Galois groups of $\mathbf{Q}^{\mathrm{ab}}$ over the fields on the left.

$$\begin{tikzcd}
\mathbf{Q}^{\mathrm{ab}} \arrow[dr, dash] & & \\
& L \cap \mathbf{Q}^{\mathrm{ab}} \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\
L \cap \mathbf{Q}^{\mathrm{ab}+} \arrow[dr, dash] & K \cap \mathbf{Q}^{\mathrm{ab}} \arrow[d, dash] & M \arrow[dl, dash] \\
& K \cap \mathbf{Q}^{\mathrm{ab}+} &
\end{tikzcd}
\qquad
\begin{tikzcd}
1 \arrow[dr, hook] & & \\
& \Gamma_L \arrow[dl, hook] \arrow[d, hook] \arrow[dr, hook] & \\
\langle \Gamma_L, -1\rangle \arrow[dr, hook] & \Gamma_K \arrow[d, hook] & \Gamma_M \arrow[dl, hook] \\
& \langle \Gamma_K, -1\rangle &
\end{tikzcd}$$

If we write Γ_M for the image of the absolute Galois group of M to $\mathrm{Aut}(\mu)$, we then get

$$E(\mu^\tau) = \left(\hat{\mathbf{Z}}^* \cap (1 + w\hat{\mathbf{Z}})\right) \Big/ \Gamma_M.$$

We conclude this chapter by computing a number of Artin densities.

Example 6.8.

Let T be the torus defined by $x^2 + 3y^2 = 1$ over $K = \mathbf{Q}$. Its splitting field is $L = \mathbf{Q}(\zeta_3)$, and $T(\mathbf{Q})$ contains non-trivial 2-torsion and 3-torsion points so w equals 6.

We take $t = 1$ in this example, and let the subgroup $V \subset T(\mathbf{Q})$ be generated by a single point x with affine coordinates $(\frac{13}{14}, \frac{3}{14})$ that as an element of L is written by

$$x^\tau = \frac{13 + 3\sqrt{-3}}{14}.$$

For the right choice of $\pi \in \mathcal{O}_L$, we have $\pi\bar{\pi} = 7$ and $x = -\pi/\bar{\pi}$.

The radical extension we work in is

$$T(\mathbf{Q}) \subset B = \langle T(\mathbf{Q}), \mu_p^\tau, \sqrt[p]{x^\tau} : p \text{ prime}\rangle.$$

For entanglement, only the primes 2, 3 and 7 matter (Theorem 6.5), and so $E(B) = E(B_{\mathrm{ab}}) = E(\mu_{21}^\tau W)$ where W is the subset of B_{ab} given by

$$W = \langle T(\mathbf{Q}), \sqrt[6]{x^\tau}\rangle.$$

When adjoining the Kummer square and cube division points of x^τ to L, we get

$$L(\sqrt{x^\tau}) = \mathbf{Q}(\zeta_3, \sqrt{-7});$$
$$L(\sqrt[3]{x^\tau}) = \mathbf{Q}(\zeta_3, \zeta_7 + \zeta_7^{-1}); \text{ and}$$
$$L(\sqrt[6]{x^\tau}) = \mathbf{Q}(\zeta_3, \zeta_7 + \zeta_7^{-1}, \sqrt{-7}) = \mathbf{Q}(\zeta_{21}).$$

These fields are extensions of degree two over the subfields obtained when we adjoin these division points to $K = \mathbf{Q}$. These subfields are additionally real because $T(\mathbf{R})$ contains p-torsion for every prime p and is divisible, and the maximal radical extension of $T(\mathbf{Q})$ is therefore contained in $T(\mathbf{R})$.

$$K(\sqrt{x^\tau}) = \mathbf{Q}(\sqrt{21});$$

$$K(\sqrt[3]{x^\tau}) = \mathbf{Q}(\zeta_7 + \zeta_7^{-1}) \cap \mathbf{R} = \mathbf{Q}(\zeta_7) \cap \mathbf{R} = \mathbf{Q}(\zeta_7)^+; \text{ and}$$
$$K(\sqrt[6]{x^\tau}) = \mathbf{Q}(\zeta_{21}) \cap \mathbf{R} = \mathbf{Q}(\zeta_{21})^+.$$

From the expression for the entanglement group $E(\mu_{21}^\tau W)$ from the start of this section, we see that it is isomorphic to

$$\mathrm{Aut}_{\mu_3}(\mu_{21})/\mathrm{im}(G_W).$$

Using the reasoning from Proposition 6.6 and Example 6.7, we can compute $\mathrm{im}(G_W)$. Using the notation from the proposition, take G to be the absolute Galois group of $K(W)$ and H the subgroup of index 2 with invariant field $L(W)$, and let φ be the natural Galois action of G on $\hat{\mu} = \bar{K}^*_{\mathrm{tors}}$. Since $K(W) \subset \mathbf{Q}^{\mathrm{ab}}$ is real and $L(W) \subset \mathbf{Q}^{\mathrm{ab}}$ is not real, the proposition states that

$\varepsilon\varphi G_W$ is isomorphic to $\mathrm{Gal}(\mathbf{Q}^{\mathrm{ab}}/L(W)) = \Gamma_{L(W)}$. When restricting that result from $\mathrm{Aut}(\hat{\mu})$ to $\mathrm{Aut}_{\mu_3}(\mu_{21})$, the image of $\Gamma_{L(W)}$ is trivial since $L(W) = \mathbf{Q}(\zeta_{21})$, so the entanglement group is isomorphic to

$$E = \mathrm{Aut}_{\mu_3}(\mu_{21}).$$

This is a cyclic group of order 6.

Recall the definition of A_p for rational primes p, with $t = 1$ and $V = \langle x \rangle$:

$$A_p = \mathrm{Aut}_{T(K)}\left(\langle T(K), \mu_p^\tau, \sqrt[p]{x^\tau}\rangle\right).$$

To compute the correction factor in the density formula, we need to compute the image of A_p in E, for $p = 2, 3, 7$.

We start with A_2. This is a group of order 2, generated by the automorphism sending $\sqrt{x^\tau}$ to $-\sqrt{x^\tau}$. We extend this to an automorphism σ of B with the identity on A_p with $p \neq 2$. This automorphism in particular fixes the elements of $\mu_7^\tau \subset B_{\mathrm{ab}}$. We shift it with a Galois element $g \in G_{\mathbf{Q}}$ with $g|_W = \sigma|_W$. Since $K(\sqrt{x^\tau}) = \mathbf{Q}(\sqrt{21})$, we see that we can choose the automorphism g acting on $L(W) = \mathbf{Q}(\zeta_{21})$ as follows.

$$\begin{aligned} g: \quad & \zeta_7 \mapsto \zeta_7^{-1} \\ & \zeta_3 \mapsto \zeta_3. \end{aligned}$$

By Corollary 2.31, the image of A_2 in E is generated by $(\sigma g^{-1})|_{\mu_{21}^\tau}$. This is

$$\langle \zeta_7^\tau \mapsto \zeta_7^{-\tau} \rangle \subset \mathrm{Aut}_{\mu_3}(\mu_{21}) = E.$$

So the image of A_2 is the unique subgroup of order 2 in E.

Next is A_3 of order 3, generated by the automorphism sending $\sqrt[3]{x^\tau}$ to $\zeta_3^\tau \sqrt[3]{x^\tau}$. We also extend this to an automorphism σ of B with the identity on A_p with $p \neq 3$. As with A_2 above, σ leaves the elements of $\mu_7^\tau \subset B_{\mathrm{ab}}$ invariant. We shift this too with a Galois element $g \in G_{\mathbf{Q}}$ with $g|_W = \sigma|_W$. Because we have $K(\sqrt[3]{x^\tau}) = \mathbf{Q}(\zeta_7)^+$, we see that, for the right choice of ζ_3^τ and ζ_7, we can pick g to act on $L(W) = \mathbf{Q}(\zeta_{21})$ as

$$\begin{aligned} g: \quad & \zeta_7 \mapsto \zeta_7^2 \\ & \zeta_3 \mapsto \zeta_3. \end{aligned}$$

Again by Corollary 2.31, the image of A_3 in E is generated by $(\sigma g^{-1})|_{\mu_{21}^\tau}$. This is now

$$\langle \zeta_7^\tau \mapsto \zeta_7^{2\tau} \rangle \subset \mathrm{Aut}_{\mu_3}(\mu_{21}) = E.$$

So the image of A_3 is the unique subgroup of order 3 in E.

We continue with A_7. The action of this automorphism group on $\sqrt[7]{x^\tau}$ has no effect on its image in the entanglement group, so we need only consider the image of

$$A_7' = \mathrm{Aut}_{T(K)}\left(\langle T(K), \mu_7^\tau \rangle\right).$$

We extend a generator of this cyclic group of order 6 to an automorphism σ of B with the identity on A_p with $p \neq 7$. Since $\langle T(K), \mu_7^\tau \rangle \cap W$ equals $T(K)$, we see that σ acts as the identity on W, so the image of A_7' in E is generated by $\sigma|_{\mu_{21}^\tau}$, which implies that the map from A_7' to E is in fact an isomorphism, and A_7 maps surjectively to E.

Since E is cyclic of order 6, its dual $E^\vee$ is also cyclic of order 6. Let χ be a generator. From the images of A_p we have determined above, we can now directly determine for which powers χ^k of χ and for which primes we have $\chi^k(A_p) = 1$, indicated by the symbol $+$ in the table below, and for which we have $\chi^k(A_p) \neq 1$, indicated by the symbol $-$. That information will then let us evaluate the density correction factor.

	2	3	7
1	$+$	$+$	$+$
χ	$-$	$-$	$-$
χ^2	$+$	$-$	$-$
χ^3	$-$	$+$	$-$
χ^4	$+$	$-$	$-$
χ^5	$-$	$-$	$-$

With $\#A_2 = 2$, and $\#A_3 = 3$ and $\#A_7 = 42$, this results in the following correction factor, using the formula from Theorem 6.4.

$$C(T, V, t) = 1 - \frac{1}{2 \cdot 41} + \frac{1}{2 \cdot 41} + \frac{1}{41} - \frac{1}{2 \cdot 41} + \frac{1}{2 \cdot 41} = \frac{42}{41}.$$

For almost all primes p we have that $\#A_p = p(p-1)$, with as the only exception $\#A_3 = 3$. Assuming GRH, this gives a density of

$$\frac{42}{41} \cdot \prod_{p \text{ prime}} \left(1 - \frac{1}{\#A_p}\right) = \frac{42}{41} \cdot \frac{4}{5} \prod_{p \text{ prime}} \left(1 - \frac{1}{p(p-1)}\right).$$

The amount of cancellation in the correction factor formula is due to the *almost* multiplicative structure of this particular table. If we were to replace the $+$ symbol in the top-right corner by a $-$ symbol, then we would be able to factor the formula for the changed correction factor C^- as follows, if we define $E_2^\vee = \{1, \chi^2, \chi^4\}$ and $E_3^\vee = \{1, \chi^3\}$.

$$C^- = \frac{-1}{\#A_7 - 1} \left(\sum_{\psi \in E_2^\vee} \prod_{\substack{p=2 \\ \psi(A_p) \neq 1}} \frac{-1}{\#A_p - 1} \right) \left(\sum_{\psi \in E_3^\vee} \prod_{\substack{p=3 \\ \psi(A_p) \neq 1}} \frac{-1}{\#A_p - 1} \right)$$

Since in fact *both* the factor for $p = 2$ and that for $p = 3$ are 0, we get $C^- = 0$. The actual correction factor C is therefore the difference between just the contribution of the top row with a $+$ symbol in the top-right in C and the contribution of the top row with a $-$ symbol in C^-. This leads, as expected, to $1 - \frac{-1}{41} = \frac{42}{41}$.

Example 6.9.

Finally, we consider an example with $t \neq 1$.

Let T again be the torus defined by $x^2+3y^2 = 1$ over $K = \mathbf{Q}$, with splitting field $L = \mathbf{Q}(\zeta_3)$ and $w = 6$.

We now take $t = 2$, and let the subgroup $V \subset T(\mathbf{Q})$ be generated by a single point $x^\tau \in T(\mathbf{Q})$, this time given with sign opposite to the previous example:

$$x^\tau = -\frac{13 + 3\sqrt{-3}}{14}.$$

So, if we choose $\pi \in \mathcal{O}_L$ right, we have $\pi\bar{\pi} = 7$ and $x = \pi/\bar{\pi}$.

In this example, the radical extensions B_p are given by

$$B_2 = \langle T(\mathbf{Q}), \mu_4^\tau, \sqrt[4]{x^\tau} \rangle; \text{ and}$$

$$B_p = \langle T(\mathbf{Q}), \mu_p^\tau, \sqrt[p]{x^\tau} \rangle \text{ for } p \text{ an odd prime.}$$

The primes that affect entanglement are again only 2, 3 and 7. We have $E(B) = E(B_{\mathrm{ab}}) = E((B_{42})_{\mathrm{ab}})$. Since x has valuation 1 at the prime π of L, we see that $(\sqrt[4]{x^\tau})^2$ is not a root of unity times an element of K^*. By the definition of B_{ab}, this implies the 4th root of x^τ is not an element of B_{ab}. So, we do not need to adjoin extra torsion division points to write $(B_{42})_{\mathrm{ab}}$ as a product of torsion division points and Kummer roots. Specifically, if we define $W = \langle T(K), \sqrt[6]{x^\tau} \rangle$, we have $(B_{42})_{\mathrm{ab}} = \mu_{84}^\tau W$.

Adjoining the Kummer square and cube division points of x^τ to L and K we get

$$L(\sqrt{x^\tau}) = \mathbf{Q}(\zeta_3, \sqrt{7});$$

$$L(\sqrt[3]{x^\tau}) = \mathbf{Q}(\zeta_3, \zeta_7 + \zeta_7^{-1}); \text{ and}$$

$$L(\sqrt[6]{x^\tau}) = \mathbf{Q}(\zeta_3, \zeta_7 + \zeta_7^{-1}, \sqrt{7}).$$

$$K(\sqrt{x^\tau}) = \mathbf{Q}(\sqrt{7});$$

$$K(\sqrt[3]{x^\tau}) = \mathbf{Q}(\zeta_7)^+; \text{ and}$$

$$K(\sqrt[6]{x^\tau}) = \mathbf{Q}(\sqrt{7}, \zeta_7 + \zeta_7^{-1}).$$

Note that as in the previous example, adjoining these points to L gives quadratic extensions of the real fields obtained by adjoining these points to K.

The entanglement group $E = E(\mu_{84}^\tau W)$ is now isomorphic to

$$\mathrm{Aut}_{\mu_3}(\mu_{84})/\mathrm{im}(G_W).$$

Using the same conclusion drawn from Proposition 6.6 in the last example, we see that the image of G_W is given by $\mathrm{Gal}(\mathbf{Q}^{\mathrm{ab}}/L(W)) = \Gamma_{L(W)}$, restricted to μ_{84}. Because $\mathbf{Q}(\mu_{84})$ is a quadratic extension of $L(W)$, the image of G_W is a group of order 2 and E is again an abelian group of order 6. The automorphism τ of $\mathbf{Q}(\mu_{84})$ that has $L(W)$ as its invariant field is given by

$$\begin{aligned} \tau: \quad \zeta_7 &\mapsto \zeta_7^{-1} \\ \zeta_3 &\mapsto \zeta_3 \\ \zeta_4 &\mapsto \zeta_4^{-1}. \end{aligned}$$

To compute the correction factor in the density formula, we need to compute the image of A_p in E, for $p = 2, 3, 7$.

The group A_2 now has order 8, but since E has a unique subgroup of order 2, the computation of the image of A_2 in the previous example almost identically applies here. That computation shows that the image of A_2 has order at least 2, which suffices to show that it has order exactly 2.

The computation for the group A_3 of order 3 proceeds exactly the same as in the last example, and we obtain that A_3 is the unique subgroup of order 3 in E.

For A_7 we again only need to consider the image of

$$A_7' = \mathrm{Aut}_{T(K)}\left(\langle T(K), \mu_7^\tau\rangle\right).$$

We extend a generator of this cyclic group of order 6 to an automorphism σ of B with the identity on A_p with $p \neq 7$. Since $\langle T(K), \mu_7^\tau\rangle \cap W$ equals $T(K)$, we see that σ acts as the identity on W, so the image of A_7' in E is generated by $\sigma|_{\mu_{84}^\tau}$. Since the unique subgroup of $\mathrm{Aut}(\mu_{84})$ maps injectively to E, the image of A_7 is at least order 3. Therefore consider σ^3. This acts on μ_{84} as follows:

$$\begin{aligned} \sigma^3: \quad \zeta_7 &\mapsto \zeta_7^{-1} \\ \zeta_3 &\mapsto \zeta_3 \\ \zeta_4 &\mapsto \zeta_4 \end{aligned}$$

This is not contained in the image of G_W which we explicitly computed above, and the map from A_7 to E is therefore surjective.

This leads to the following table.

	2	3	7
1	+	+	+
χ	−	−	−
χ^2	+	−	−
χ^3	−	+	−
χ^4	+	−	−
χ^5	−	−	−

Because of the same cancellation as in the previous example, the correction factor is again

$$C(T, V, t) = \frac{42}{41}.$$

For almost all primes p we have that $\#A_p = p(p-1)$, with as the only exception $\#A_2 = 8$ and $\#A_3 = 2$. Assuming GRH, this gives a density of

$$\frac{42}{41} \cdot \prod_{p \text{ prime}} \left(1 - \frac{1}{\#A_p}\right) = \frac{42}{41} \cdot \frac{7}{4} \cdot \frac{4}{5} \prod_{p \text{ prime}} \left(1 - \frac{1}{p(p-1)}\right).$$