The norm torus

Joshua Ruiter

November 26, 2019

These notes were prepared for a seminar talk given at the student algebra seminar at Michigan State University on November 18th, 2019. The most helpful sources in preparing were Milne’s notes on algebraic groups, and notes from a class on algebraic groups taken at MSU the previous summer with professor Rajesh Kulkarni. Thanks also to my advisor Igor Rapinchuk for answering several clarifying questions.

Contents

1 Background/setup material ................................. 2
   1.1 Review of last week .................................. 2
   1.2 Kernels of morphisms of algebraic groups .......... 2
   1.3 Tori .............................................. 2

2 The norm torus .............................................. 3
   2.1 Generalized norm map on $K^{\text{sep}}$-points ......... 3
   2.2 Examples of norm tori ................................ 6

3 Characters .................................................. 8
   3.1 Non-splitting of norm torus ......................... 8
1 Background/setup material

1.1 Review of last week

Definition 1.1. Let \( K \) be a field. An affine algebraic \( K \)-group is a representable covariant functor \( G : \text{Alg}_K \to \text{Gp} \). A morphism of algebraic \( K \)-groups is a natural transformation.

Example 1.2. For any field, we have an algebraic \( K \)-group \( \mathbb{G}_m = \mathbb{G}_m^K \), given by \( \mathbb{G}_m(A) = A^\times \).

Definition 1.3. Given a field extension \( L/K \) and an algebraic \( L \)-group \( G \), the Weil restriction of \( G \) is the algebraic \( K \)-group \( R_{L/K}G \) defined by

\[
R_{L/K}G(A) = G(A \otimes_K L) = G(A_L)
\]

In particular, \( R_{L/K}G(K) = G(L) \).

Definition 1.4. Let \( L/K \) be a finite extension. For a \( K \)-algebra \( A \), let \( \ell : A_L^\times \to \text{GL}_A(A_L) \) be the left regular representation, and \( \text{det} : \text{GL}_A(A_L) \to A^\times \) be the determinant map. Define

\[
N_A = \text{det} \circ \ell : A_L^\times \to A^\times
\]

Proposition 1.5. Let \( L/K \) be a finite extension. The group homomorphisms \( N_A \) above give a morphism of algebraic groups \( R_{L/K} \mathbb{G}_m \to \mathbb{G}_m^K \) with the property that taking \( K \)-points gives the usual field norm map \( N_L^K : L^\times \to K^\times \).

1.2 Kernels of morphisms of algebraic groups

Definition 1.6. Let \( \eta : G \to H \) be a morphism of algebraic \( K \)-groups, so for every \( K \)-algebra \( A \) we have a group homomorphism \( \eta_A : G(A) \to H(A) \). For a \( K \)-algebra \( A \), define

\[
(ker \eta)(A) = \ker(\eta_A)
\]

This makes \( \ker \eta \) into an algebraic \( K \)-group.

Remark 1.7. The “right” way to define the kernel is by the usual categorical universal property, and then to show that such objects exist in the category of algebraic groups, and then to show that that object is the one I just described. But this is a seminar talk, so no time for that.

1.3 Tori

Definition 1.8. Let \( T \) be an affine algebraic \( K \)-group, and let \( \overline{K} \) be the algebraic closure of \( K \). \( T \) is a \( K \)-torus if \( T(\overline{K}) \cong (\overline{K}^\times)^r \) for some \( r \in \mathbb{Z}_{\geq 0} \). The number \( r \) is called the rank or absolute rank of the torus \( T \).

Example 1.9. \( \mathbb{G}_m^K \) is a \( K \)-torus of rank 1. More generally, \( (\mathbb{G}_m)^r \) is a \( K \)-torus of rank \( r \).
Example 1.10. Let $K$ be a field, and view $\text{GL}_n$ as an algebraic $K$-group. Inside of $\text{GL}_n$ is the diagonal subgroup.

$$D_n : \text{Alg}_K \to \text{Gp} \quad A \mapsto D_n(A) = \left\{ \begin{pmatrix} a_1 & \cdots & a_n \end{pmatrix} : a_i \in A^\times \right\}$$

There is an isomorphism $D_n \cong (\mathbb{G}_m)^n$, so $D_n$ is a $K$-torus of rank $n$. On $A$-points, the isomorphism is

$$(\mathbb{G}_m)^n(A) \xrightarrow{\cong} D_n(A) \quad (a_1, \ldots, a_n) \mapsto \text{diag}(a_1, \ldots, a_n)$$

In particular, it is a torus inside of $\text{GL}_n$.

Remark 1.11. In the study and classification of algebraic groups, subgroups of a given algebraic group which are tori play a very important role in understanding the structure of that group, but we don’t have time to get into this at the moment.

Definition 1.12. Let $T$ be a $K$-torus of rank $r$. $T$ is called split if $T(K) \cong (K^\times)^r$. If $T$ is not split, it is called non-split.

Example 1.13. It is not that easy to give examples of non-split tori. By the end of these notes, the goal is to see that the kernel of the norm map $N : R_{L/K} \mathbb{G}_m^L \to \mathbb{G}_m^K$ is a non-split torus, at least when $L/K$ is Galois.

2 The norm torus

2.1 Generalized norm map on $K^{\text{sep}}$-points

In order to define the norm torus, I’m going to need to work out some things about what the generalized norm map does on $K^{\text{sep}}$-points. We want to describe the map

$$N_{K^{\text{sep}}} : (K^{\text{sep}} \otimes_K L)^\times \to K^{\text{sep}}^\times$$

The first step is to describe the domain of this map in better terms.

Lemma 2.1. Let $L/K$ be a finite separable extension of degree $d = [L : K]$, and let $K^{\text{sep}}$ be the separable closure of $K$. Then

$$K^{\text{sep}} \otimes_K L \cong (K^{\text{sep}})_d$$

In particular,

$$(K^{\text{sep}} \otimes_K L)^\times \cong (K^{\text{sep}}^\times)_d$$

Proof. By the primitive element theorem, $L = K(\alpha)$ for some $\alpha \in L$. Let $g \in K[x]$ be the minimal polynomial of $\alpha$, so that $\deg g = d$ and we have an isomorphism of $K$-algebras

$$L = K(\alpha) \cong \frac{K[x]}{(g)}$$
Then we may write
\[ g(x) = \prod_{i=1}^{d} (x - \beta_i) \]
where \( \beta_i \in E \), and the \( \beta_i \) are all Galois conjugates. Viewing \( K_{\text{sep}} \) as a \( K \)-algebra, we have
\[ K_{\text{sep}} \otimes_K L \cong K_{\text{sep}} \otimes \frac{K[x]}{(g)} \cong \frac{K_{\text{sep}}[x]}{(g)} \cong \frac{K_{\text{sep}}[x]}{((x - \beta_1) \cdots (x - \beta_d))} \]
(These are all isomorphisms of \( K \)-algebras.) Since the elements \( \beta_1, \ldots, \beta_d \) are distinct, the ideals \( (x - \beta_1), \ldots, (x - \beta_d) \) are pairwise coprime, so by the Chinese Remainder Theorem the above we have
\[ \frac{K_{\text{sep}}[x]}{((x - \beta_1) \cdots (x - \beta_d))} \cong \frac{K_{\text{sep}}[x]}{(x - \beta_1)} \times \cdots \times \frac{K_{\text{sep}}[x]}{(x - \beta_d)} \]
Once again, this is an isomorphism of \( K \)-algebras. On the right side, each factor is isomorphic to \( K_{\text{sep}} \), hence
\[ K_{\text{sep}} \otimes_K L \cong (K_{\text{sep}})^d \]

**Remark 2.2.** The previous lemma may be generalized by replacing \( K_{\text{sep}} \) by any separable extension of \( K \) over which \( g \) splits completely. In particular, there is a minimal such \( E \), which is finite over \( K \).

**Example 2.3** (Weil restriction for \( \mathbb{G}_m \)). Let \( L/K \) be a finite field extension of degree \( d = [L : K] \), and let \( G = \mathbb{G}_m \) be the algebraic \( L \)-group defined previously, with \( \mathbb{G}_m(A) = A^\times \). The Weil restriction of \( \mathbb{G}_m \) is \( R_{L/K}\mathbb{G}_m \). For a \( K \)-algebra \( A \), the group of \( K \)-points of \( R_{L/K}\mathbb{G}_m \) is
\[ R_{L/K}\mathbb{G}_m(A) \cong \mathbb{G}_m(A_L) = A_L^\times \]
In the case \( A = K_{\text{sep}} \), by the previous lemma,
\[ R_{L/K}\mathbb{G}_m(K_{\text{sep}}) = \mathbb{G}_m(K_{\text{sep}} \otimes_K L) = (K_{\text{sep}} \otimes_K L)^\times \cong (K_{\text{sep}}^\times)^d \]

**Remark 2.4.** Suppose \( L/K \) is Galois of degree \( d = [L : K] \), and let \( K_{\text{sep}} \) be the separable closure, with a fixed embedding \( \iota : K \hookrightarrow K_{\text{sep}} \). In the previous lemma, we fully described the unit group of \( K_{\text{sep}} \otimes_K L \).
\[ K_{\text{sep}} \otimes_K L \cong (K_{\text{sep}})^d \quad (K_{\text{sep}} \otimes_K L)^\times \cong (K_{\text{sep}}^\times)^d \]
Using naturality of the generalized norm applied to \( \iota \), we get the following commutative diagram.
\[
\begin{array}{ccc}
L^\times & \xrightarrow{N_K^L} & K^\times \\
\downarrow{\iota \otimes 1} & & \downarrow{\iota} \\
(K_{\text{sep}}^\times)^d & \xrightarrow{N_{K_{\text{sep}}}^L} & K_{\text{sep}}^\times \\
\end{array}
\]

\(^1I\) think it is only necessary to assume \( L/K \) is separable for this whole remark, but I am not sure.
The vertical map on the left is somewhat mysterious, since it involves several isomorphisms, include isomorphisms coming from the Primitive Element Theorem and the Chinese Remainder Theorem. If follow through all the isomorphisms, is can be described very nicely as
\[ L^\times \to (K_{\text{sep}}^\times)^d \quad \lambda \mapsto (\sigma_1 \lambda, \ldots, \sigma_d \lambda) \]

On the other hand, what can we say about the bottom horizontal map, \( N_{K_{\text{sep}}} \)? The left regular representation of \((K_{\text{sep}}^\times)^d\) is just
\[ (K_{\text{sep}}^\times)^d \to \text{GL}_{K_{\text{sep}}}((K_{\text{sep}})^d) \quad (\sigma_1, \ldots, \sigma_d) \mapsto \text{diag}(\sigma_1, \ldots, \sigma_d) \]

Taking the determinant of a diagonal matrix is just taking the product, so the norm map \( N_{K_{\text{sep}}} \) is just given by
\[ N_{K_{\text{sep}}} : (K_{\text{sep}}^\times)^d \to K_{\text{sep}}^\times \quad (\sigma_1, \ldots, \sigma_d) \mapsto \prod_{i=1}^{d} \sigma_i \]

Hence the commutative diagram above says that
\[ N_{K_{\text{sep}}} (\sigma_1 \lambda, \ldots, \sigma_d \lambda) = \prod_{i=1}^{d} \sigma_i = N_{L_{\text{sep}}} (\lambda) \]

which is a fact we already knew about the regular field norm, when \( L/K \) is Galois.

For the next proposition, recall that every extension of a perfect field is separable.

**Proposition 2.5.** Let \( K \) be a perfect field, and let \( L/K \) be a finite Galois2 extension of degree \( d = [L : K] > 1 \), and let \( N : R_{L/K} \mathbb{G}_m \to \mathbb{G}_m \) be the norm. Let \( T \) be the kernel of \( N \). Then \( T \) is a torus. In particular, \( T(K_{\text{sep}}) \cong (K_{\text{sep}}^\times)^{d-1} \).

**Proof.** As \( K \) is perfect, \( \overline{K} = K_{\text{sep}} \). First we verify that \( T \) is a torus, by computing its group of \( K_{\text{sep}} \) points.
\[ T(K_{\text{sep}}) = \ker N_{K_{\text{sep}}} \]

By the previous remark \[2.4 \] the map \( N_{K_{\text{sep}}} \) is just
\[ N_{K_{\text{sep}}} : (K_{\text{sep}}^\times)^d \to K_{\text{sep}}^\times \quad (\alpha_1, \ldots, \alpha_d) \mapsto \prod_{i=1}^{d} \sigma_i \]

hence
\[ T(K_{\text{sep}}) = \left\{ (\alpha_1, \ldots, \alpha_d) \in (K_{\text{sep}}^\times)^d : \alpha_1 \cdots \alpha_d = 1 \right\} = \{ (\alpha_1, \ldots, \alpha_{d-1}, \sigma_d) \in (K_{\text{sep}}^\times)^d : \alpha_d = \alpha_1^{-1} \cdots \alpha_{d-1}^{-1} \} \cong \{ (\alpha_1, \ldots, \alpha_{d-1}) \in (K_{\text{sep}}^\times)^{d-1} \} = (K_{\text{sep}}^\times)^{d-1} \]

Hence \( T \) is a torus. \( \square \)

**Definition 2.6.** We will call the kernel of the norm the **norm torus** from now on.

**Remark 2.7.** The next goal is to show that the norm torus is not split (over the base field \( K \)). We won’t actually prove it today, but we’ll do several examples, and then talk about some theory of characters which would be a step towards the proof.

---

2I think it is is only necessary to assume \( L/K \) is separable for this, but I am not sure.
2.2 Examples of norm tori

Now we give several worked examples of the norm torus. We describe the points of $T$ over the base field, and show that $T$ is non-split, when possible.

**Example 2.8** (Norm torus for $\mathbb{C}/\mathbb{R}$). Let $L/K = \mathbb{C}/\mathbb{R}$, which is Galois of degree 2. We have the norm map

$$N : R_{C/R} \mathbb{G}_m^C \to \mathbb{G}_m^R$$

and as before let $T = \ker N$ be the norm torus, so $T$ is an algebraic $\mathbb{R}$-group. We already know that $T$ is a torus, but let’s just verify by taking $\mathbb{C}$-points.

$$R_{C/R} \mathbb{G}_m^C(\mathbb{C}) = (\mathbb{C} \otimes \mathbb{C})^\times \cong (\mathbb{C}^\times)^2$$

$$\mathbb{G}_m^R(\mathbb{C}) = \mathbb{C}^\times$$

$$N_C : \mathbb{C}^\times \to \mathbb{C}^\times \quad (z, w) \mapsto zw$$

$$T(\mathbb{C}) = \ker N_C = \{ (z, z^{-1}) : z \in \mathbb{C}^\times \} \cong \mathbb{C}^\times$$

Let’s take a moment to be explicit about the isomorphism $\mathbb{C} \otimes \mathbb{C} \cong (\mathbb{C}^\times)^2$, since it quite as simple as one would like. One explicit isomorphism is given by

$$\mathbb{C} \otimes \mathbb{C} \to (\mathbb{C}^\times)^2 \quad z \otimes w \mapsto (zw, zw)$$

Now let’s take $\mathbb{R}$-points of the torus $T$, where we get the usual field norm.

$$R_{C/R} \mathbb{G}_m^C(\mathbb{R}) = (\mathbb{R} \otimes \mathbb{C})^\times = \mathbb{C}^\times$$

$$\mathbb{G}_m^R(\mathbb{R}) = \mathbb{R}^\times$$

$$N_R : \mathbb{C}^\times \to \mathbb{R}^\times \quad z = x + iy \mapsto N_R^C(z) = |z| = x^2 + y^2$$

$$T(\mathbb{R}) = \ker N_R = \{ z \in \mathbb{C}^\times : |z| = 1 \} \cong S^1$$

So $T$ is split over $\mathbb{R}$ if and only if $\mathbb{R}^\times \cong S^1$. These are clearly not isomorphic groups, since $S^1$ has 4-torsion ($i^4 = 1$) but $\mathbb{R}^\times$ has no 4-torsion (the only torsion in $\mathbb{R}^\times$ is order 2, ±1). Hence $T$ is non-split.

**Remark 2.9.** I think the previous example is the primary motivation for using the word “torus” when talking about these special algebraic groups. In particular, if we take two copies of the previous example,

$$N_R \times N_R : \mathbb{C}^\times \times \mathbb{C}^\times \to \mathbb{R}^\times \times \mathbb{R}^\times$$

the kernel is $S^1 \times S^1$, which is what algebraic topologists mean by the word “torus.”

**Example 2.10** (Norm torus for quadratic extension). We can generalize the previous example to an arbitrary quadratic extension of a perfect field. Let $K$ be a perfect field, and $L/K$ a quadratic extension. So we can write $L$ as $L = K(\sqrt{d})$ where $d$ is some non-square in $K$.

The previous example was just the case $d = -1 \in \mathbb{R}$, but now we’re considering things like quadratic extensions of $\mathbb{Q}$ at the same time. Note that every quadratic extension is Galois.
We already know what happens when we take $K^{\text{sep}}$ points in general, so let’s just focus on taking $K$-points. Fix the $K$-basis $B = \{1, \sqrt{d}\}$ of $L$, and let us describe the left regular representation of $L$ in terms of this basis.

\[
\ell_1(a + b\sqrt{d}) = a + b\sqrt{d} = \begin{pmatrix} a \\ b \end{pmatrix}_B
\]

\[
\ell_{\sqrt{d}}(a + b\sqrt{d}) = a\sqrt{d} + bd = \begin{pmatrix} bd \\ a \end{pmatrix}_B
\]

So we can describe the left regular representation of $L$ by

\[
\ell : L^\times \to \text{GL}_2(K) \quad a + b\sqrt{d} \mapsto \begin{pmatrix} a & bd \\ b & a \end{pmatrix}
\]

And composing with determinant we get the $K$-points of the norm map $N$.

\[
N_K = N^L_K : L^\times \to K^\times \quad a + b\sqrt{d} \mapsto a^2 + db^2
\]

In this scenario, the left regular representation of $L$ is an embedding, so we may identify $L^\times$ with its image in $\text{GL}_2(K)$.

\[
L^\times = (K(\sqrt{d})^\times \cong \left\{ \begin{pmatrix} a & bd \\ b & a \end{pmatrix} : a, b \in L, \text{not both zero} \right\} \subset \text{GL}_2(K)
\]

Using this identification, $K$-points of the norm torus (the kernel of $N^L_K$) is just the intersection of this subgroup with $\text{SL}_2(K)$.

\[
T(K) = \ker N^L_K = \left\{ \begin{pmatrix} a & bd \\ b & a \end{pmatrix} : a, b \in L, \text{not both zero}, a^2 + bd^2 = 1 \right\} \subset \text{SL}_2(K)
\]

I don’t know how to justify the assertion $T(K) \not\cong K^\times$, to show that $T$ is non-split in this case.

**Example 2.11.** Let $K = \mathbb{F}_q$ be the finite field with $q$ elements, and let $L = \mathbb{F}_{q^d}$ be the unique extension of $K$ of degree $d$. Let $T$ be the associated norm torus, and let us describe the $K$-points of $T$. Recall that the multiplicative group of a finite field is cyclic, and that the usual field norm map between finite fields is always surjective.

\[
\mathbb{G}_m(\mathbb{F}_q) = \mathbb{F}_q^\times \cong \mathbb{Z}/(q-1)\mathbb{Z}
\]

\[
R_{\mathbb{F}_{q^d}/\mathbb{F}_q} \mathbb{G}_m(\mathbb{F}_q) = (\mathbb{F}_{q^d})^\times \cong \mathbb{Z}/(q^d-1)\mathbb{Z}
\]

\[
N_{\mathbb{F}_{q^d}} : \mathbb{Z}/(q^d-1)\mathbb{Z} \to \mathbb{Z}/(q-1)\mathbb{Z}
\]

Just from knowing we have a surjective homomorphism of cyclic groups, we know that the kernel must be cyclic of order $q^d - 1 = 1 + q + \cdots + q^{d-1}$. Thus

\[
T(\mathbb{F}_q) \cong \mathbb{Z}/(1 + \cdots + q^{d-1})\mathbb{Z}
\]

Hence $T$ is split if and only if $1 + q + \cdots q^{d-1} = q - 1$. This is clearly impossible for any $q$, since it is equivalent to $1 + q^2 + \cdots + q^{d-1} = -1$. Hence $T$ is non-split.
3 Characters

Definition 3.1. Let $G$ be an affine algebraic $K$-group. A character of $G$ is a homomorphism (of affine algebraic groups) $\chi : G \to \mathbb{G}_m$. The characters of $G$ themselves form an abelian group, and the character group $X(G)$ is the group of such characters.

$$X(G) = \text{Hom}(G, \mathbb{G}_m)$$

Let’s say a little more about how the characters form a group. Given two characters (natural transformations) $\chi, \chi' : G \to \mathbb{G}_m$, we need to describe $\chi + \chi' : G \to \mathbb{G}_m$. Given a $K$-algebra $A$, we have homomorphisms $\chi_A, \chi'_A : G(A) \to \mathbb{G}_m(A)$ so we just define $(\chi + \chi')_A$ by

$$(\chi + \chi')_A = \chi_A + \chi'_A : G(A) \to \mathbb{G}_m(A) \quad (\chi + \chi')_A(x) = \chi_A(x) \cdot \chi'_A(x)$$

where $\cdot$ denotes multiplication in $\mathbb{G}_m(A) = A^\times$.

Example 3.2 (Character group of $\mathbb{G}_m$). Consider the affine algebraic $K$-group $\mathbb{G}_m = \mathbb{G}_m^K$. We show that the character group of $\mathbb{G}_m$ is $\mathbb{Z}$. By the Yoneda lemma,

$$\text{Hom}(\mathbb{G}_m, \mathbb{G}_m) \cong \text{Hom}_{\text{Alg}_K}(K[x, x^{-1}], K[x, x^{-1}])$$

Let $\alpha : K[x, x^{-1}] \to K[x, x^{-1}]$ be a $K$-algebra homomorphism, so it is determined by the value of $x$. So let

$$\alpha(x) = \frac{f(x)}{x^n}$$

where $f \in K[x]$ is some polynomial and $n \in \mathbb{Z}$. Since $x$ is a unit in $K[x, x^{-1}]$, $\alpha(x)$ is also a unit in $K[x, x^{-1}]$, hence

$$\alpha(x)^{-1} = \frac{x^n}{f(x)} \in K[x, x^{-1}]$$

so $f(x)$ cannot have any nonzero roots in $K$. Hence $f(x) = ax^m$ for some $a \in K^\times, m \in \mathbb{Z}$. Thus $\alpha(x) = ax^{m-n} = ax^t$ for some $a \in K, t \in \mathbb{Z}$. Since $\alpha$ is a $K$-algebra homomorphism, $\alpha(1) = 1$, so $a = 1$. Hence $\alpha(x) = x^t$ for some $t \in \mathbb{Z}$. Hence

$$\mathbb{Z} \mapsto \text{Hom}_{\text{Alg}_K}(K[x, x^{-1}], K[x, x^{-1}]) \quad t \mapsto (x \mapsto x^t)$$

is a group isomorphism, so

$$\text{Hom}(\mathbb{G}_m, \mathbb{G}_m) \cong \mathbb{Z}$$

3.1 Non-splitting of norm torus

Proposition 3.3. Let $T$ be a $K$-torus of rank $r$. Then $X(T)$ is free abelian, and $T$ is split if and only if $X(T)$ is free abelian of rank $r$.

Proof. Omitted.

Proposition 3.4. Let $K$ be a perfect field, and let $L/K$ be a finite Galois extension of degree $d = [L : K] > 1$, and let $T$ be the associated norm torus. Then $X(T)$ is free abelian of rank less than $d - 1$; hence $T$ is non-split.

Proof. Involves theory of characters, not enough time.