Generic Norm One Tori

Lieven Le Bruyn*

Department of Mathematics
and Computer Science
University of Antwerp, UIA

March 1990 - 90-04

Abstract

A Hilbert parametrization is given for the norm one elements of a generic field extension of prime degree. It is also shown that these norm one tori are seldom k-rational.

Keywords

Norm one elements, Rationality problems

AMS-classification

14M20

---

* Supported by an NFWO-grant

Generic Norm One Tori

Lieven Le Bruyn*
Department Mathematics
Universitaire Instelling Antwerpen

March 6, 1990

1 Introduction

In this note we aim to study the norm-one torus $R^1_{K/k}\mathbb{G}_m$ of a finite separable fieldextension K/k of degree n. If K/k is a cyclic Galois extension one can show that $R^1_{K/k}\mathbb{G}_m$ is a k-rational variety. Moreover, the archetype version of Hilbert 90 tells us that all its k-rational points can be written as $\frac{\alpha}{\sigma.\alpha}$ where $\alpha \in K^*$ and σ a generator of $Gal(K/k)$. If K/k is Galois but no longer (meta)cyclic, finding parametrizations of all k-rational points in $R^1_{K/k}\mathbb{G}_m$ usually is a rather hopeless task as the following example due to Colliot-Thélène and Sansuc [3,p.207] shows : let $K = \mathbb{Q}(\sqrt{2}, \sqrt{p_1 \ldots p_{2n+1}})$ where the p_i are distinct prime numbers congruent to 3 modulo 8,then $K/\mathbb{Q}$ is Galois with group V_4 but there are 2^{2n+1} different classes of $\mathbb{Q}$-rational points on $R^1_{K/\mathbb{Q}}\mathbb{G}_m$ under Manin's R-equivalence,see [5] or [3].

The situation becomes even more complicated in case K/k is no longer Galois, see [3.p.209-212] for some of the rare manageable cases. In this note we will study the generic case i.e. K/k is separable of degree n such that the Galois closure L has group S_n. Let us give an easy example : take $K = \mathbb{Q}(\sqrt[3]{2})$ over $\mathbb{Q}$, then $L = \mathbb{Q}(\sqrt[3]{2}, i\sqrt{3})$ and $Gal(L/\mathbb{Q}) = S_3$. Then $R^1_{K/\mathbb{Q}}\mathbb{G}_m$ is determined by the equation

$$x^3 + 2y^3 + 4z^3 - 6xyz = 1 \qquad (1)$$

*supported by an NFWO- grant

As S_3 is a dihedral group we can apply [4,II.1.c] and obtain that $R^1_{K/\mathbb{Q}}\mathbb{G}_m$ is $\mathbb{Q}$-rational and that there exists a Hilbert-like parametrization of the $\mathbb{Q}$-rational points. To be precise, $\zeta \in K^*$ has norm one iff $\zeta = N_{L/K}(\alpha)$ for some $\alpha \in L^*$ where $N_{L/K}$ is the norm-map.

We will show that the situation becomes more complicated if n increases : $R^1_{K/k}\mathbb{G}_m$ is no longer k-rational if $n = [K : k] \geq 4$ (at least for prime and non-squarefree vallues of n). Still, for prime degree extensions it is possible to determine all k-rational points of $R^1_{K/k}\mathbb{G}_m$ by a Hilbert-like procedure, i.e. they are all of the form $N_{K'/K}(\frac{\alpha}{(12).\alpha})$ where $K' = L^{S_{n-2}}$. However this result does not generalize to composite degrees if k is a global field.

As some of these results are sort of dual to some of [1] we will merely sketch the main ideas and refer the reader to loc.cit. for more details.

Acknowledgement

Thanks are due to Christine Bessenrodt for allowing me to incorporate some arguments which were left out of the final version of [1] and to Jean-Louis Colliot-Thélène for valuable suggestions and references.

2 Non-rationality of $R^1_{K/k}\,\mathbb{G}_m$

Let K/k be a finite separable extension and X a (quasi-projective) K-variety,then with $R_{K/k}X$ we denote the Weil descent k-variety obtained from X. It is characterized as the representable functor which assigns to a commutative k-algebra A :

$$R_{K/k}X(A) = X(A \otimes_k K) \tag{2}$$

Let $\mathbb{G}_{m,k}$ be the multiplicative group over k, then an algebraic k-torus T is an algebraic k-group such that $T \times_k k_s \simeq \mathbb{G}^r_{m,k_s}$ where k_s is the separable closure of k. A typical example is the torus $R_{K/k}\,\mathbb{G}_m$ whose underlying variety is the open subvariety of $R_{k,k}\,\mathbb{A}^1 = \mathbb{A}^n_k$ consisting of the points x s.t. $N_{K/k}(x) \neq 0$. We say that an algebraic k-torus T is split by a Galois extension L/k iff $T \times_k L \simeq \mathbb{G}^r_{m,L}$. For example $R_{K/k}\,\mathbb{G}_m$ and $R^1_{K/k}\mathbb{G}_m$ (which is the kernel of the norm-map $R_{K/k}\,\mathbb{G}_m \to \mathbb{G}_m$) are split by the Galois closure L of K/k. There is a natural anti-equivalence of categories between the algebraic k-tori split by L and the $\mathbb{Z}G$-lattices of finite rank where $G = Gal(L/k)$ obtained by associating to a torus T its lattice of characters $\hat{T}$. Under this equivalence $\mathbb{G}_m$ corresponds to the trivial G-lattice $\mathbb{Z}$, $R_{K/k}\,\mathbb{G}_m$ to the permutation lattice $\mathbb{Z}G/H$ where H is the subgroup of G s.t. $L^H = K$ and $R^1_{K/k}\mathbb{G}_m$ to $J_{G/H}$ which is determined by the sequence

$$0 \rightarrow \mathbb{Z} \rightarrow \mathbb{Z}G/H \rightarrow J_{G/H} \rightarrow 0 \tag{3}$$

the first map being the norm map $1 \rightarrow \sum gH$. Brylinski [2] obtained an algorithmic procedure to construct a smooth proper equivariant k-model X_T of a given algebraic k-torus T. The embedding $T \hookrightarrow X_T$ gives rise to an exact sequence of $\mathbb{Z}G$-lattices

$$0 \rightarrow \hat{T} \rightarrow Div_{Y\times_k K}(X_T \times_k K) \rightarrow Pic(X_T \times_k K) \rightarrow 0 \tag{4}$$

where Y is the closed subvariety complementary to T. Further, it is easy to see that the middle term is a permutation $\mathbb{Z}G$-lattice and that the Picard group is a flasque $\mathbb{Z}G$-lattice meaning that $\hat{H}^{-1}(G', Pic(X_T \times_k K)) = 0$ for all subgroups G' of G.

Voskresenskii [7] proved that if the torus T is k-rational then the $\mathbb{Z}G$-lattice $Pic(X_T \times_k K)$ is a stable permutation $\mathbb{Z}G$- lattice i.e. there exist permutation lattices P_1 and P_2 such that

$$Pic(X_T \times_k K) \oplus P_1 \simeq P_2 \tag{5}$$

We are now in a position to state and prove :

Theorem 1 *If K/k is a finite separable fieldextension of prime degree p with Galois closure L with group S_p, then the norm-one torus $R^1_{K/k}\mathbb{G}_m$ is not k-rational unless $p \leq 3$.*

Proof : (compare with [1,Cor 1]) Let X be a smooth model of $R^1_{K/k}\mathbb{G}_m$, then we have to show that $Pic(X \times_k K)$ cannot be a stable permutation $\mathbb{Z}S_p$-lattice. We have an exact sequence of $\mathbb{Z}S_p$-lattices

$$0 \rightarrow J_{S_p/S_{p-1}} \rightarrow \mathbb{Z}S_p/S_{p-2} \rightarrow M_p \rightarrow 0 \tag{6}$$

where the lefthand map is induced from the $\mathbb{Z}S_p/S_{p-1} \rightarrow \mathbb{Z}S_p/S_{p-2}$ sending x_i to $\sum_j (y_{ij} - y_{ji})$ where the x_i (resp y_{ij}) are the canonical basevectors of the permutation lattices $\mathbb{Z}S_p/S_{p-1}$ (resp. $\mathbb{Z}S_p/S_{p-2}$). We claim that M_p is a flasque lattice, in fact even an invertible one (i.e. a direct summand of a permutation lattice). This is verified locally : over primes $q \neq p$ the above sequence as well as the one defining $J_{S_p/S_{p-1}}$ splits and for the prime p we have

$$\widehat{\mathbb{Z}_p} \otimes M_p \simeq \Omega^{-2}(\widehat{\mathbb{Z}_p}) \oplus \mathbb{P} \tag{7}$$

where $\mathbb{P}$ is projective (hence invertible) and as the Sylow p-subgroup of S_p is cyclic $\Omega^{-2}(\widehat{\mathbb{Z}_p})$ in invertible too,proving our claim (using duality and Shapiro's lemma). Now, using flasque-ness of M_p and $Pic(X \times_k K)$ one easily sees that

$$M_p \oplus Div_{Y \times_k K}(X \times_k K) \simeq Pic(X \times_k K) \oplus \mathbb{Z}S_p/S_{p-2} \tag{8}$$

whence we have to show that M_p cannot be stable permutation. This can be tested locally. Now, p-locally we can use Green-correspondence to reduce the problem to a finite representation-type setting (over the p-hypoelementary subgroup $N_p = N_{S_p}(Syl_p(S_p))$) which enables us to show that

$$\bigoplus_{i=1,(i,p-1)=1}^{\frac{p-1}{2}} (\Omega^{2i}(\widehat{\mathbb{Z}_p}) \oplus \Omega^{-2i}(\widehat{\mathbb{Z}_p})) \tag{9}$$

is stable permutation and no proper subsum is. This, combined with the fact that projectives $\widehat{\mathbb{Z}_p}S_p$-lattices are stable permutation finishes the proof. □

A cohomological argument due to Snider and Saltman shows that a similar statement holds for all non-squarefree degrees. Of course, one may conjecture that $R^1_{K/k}\mathbb{G}_m$ can never be k-rational provided the degree is larger than 4 (with the possible exception of 6).

3 Rational points of $R^1_{K/k}\,\mathbb{G}_m$

The foregoing result may suggest that it is rather hard to find an explicit Hilbert-like parametrization of all k-rational points on $R^1_{K/k}\mathbb{G}_m$. However, a result of Colliot-Thélène and Sansuc [8,Prop.9.1] offers some hope. They show that $Pic(X \times_k K)$ is a direct factor of a permutation lattice. As in the proof of the next result this essentially shows that a Hilbert-like parametrization of the norm one elements is possible. However, their general principle usually gives a too large permutation middle term on which the following result improves drastically :

Theorem 2 *Let K/k be a separable fieldextension of prime degree p with Galois closure L with group S_p. Then,all k- rational points on $R^1_{K/k}\mathbb{G}_m$ (or,alternatively,all norm one elements of K^*) can be written as*

$$N_{K'/K}(\frac{\alpha}{(12...p).\alpha}) \tag{10}$$

where $\alpha \in K^*$ and $K' = L^{S_{n-2}}$.

Proof : (compare with [1,Prop.3]) Let T_p be the k-torus corresponding to the invertible $\mathbb{Z}S_p$-lattice M_p. Then we have an exact sequence of tori

$$1 \to T_p \to R_{K'/k}\,\mathbb{G}_m \to R^1_{K/k}\mathbb{G}_m \to 1 \tag{11}$$

Taking global sections (over k) gives us an exact sequence

$$K'^* \to R^1_{K/k}\mathbb{G}_m(k) \to H^1(\mathcal{G}, T_p(k_s)) \to H^1(\mathcal{G}, R_{K'/k}\mathbb{G}_m(k_s)) \tag{12}$$

where $\mathcal{G} = Gal(k_s/k)$. Now, for any fieldextension $k \subset M \subset k_s$ we have that $H^1(Gal(k_s/k), R_{M/k}\,\mathbb{G}_m(k_s)) = H^1(Gal(k_s/M), k_s^*) = 0$ by Hilbert 90. So, the last term vanishes and also the next to last as we have a torus S_p s.t.

$$T_p \times_k S_p \cong \times_i R_{K_i/k}\,\mathbb{G}_m \tag{13}$$

Hence, the map $K'^* \to R^1_{K/k}\mathbb{G}_m(k)$ is surjective which proves the result taking into account that this map comes from the dual map between the character lattices which was induced from $\mathbb{Z}S_p/S_{p-1} \to \mathbb{Z}S_p/S_{p-2}$ sending x_i to $\sum_j(y_{ij} - y_{ji})$. □

Clearly, for any degree n, elements of K of the form $N_{K'/K}(\frac{\alpha}{(12).\alpha})$ are of norm one. However, if n is composite there may be others :

Theorem 3 *Let K/k be a finite separable fieldextension of degree n of numberfields, s.t. the Galois closure L has group S_n. If n is composite, then the cokernel of the map*

$$N_{K'/K}(\frac{\alpha}{(12).\alpha}) : K'^* \to R^1_{K/k}\mathbb{G}_m(k) \tag{14}$$

where $K' = L^{S_{n-2}}$ is infinite.

Proof : The Tate-Nakayama exact sequence gives us

$$0 \to TS^1(T_n) \to H^1(S_n, T_n(L)) \to \oplus H^1(S_{n,v}, T_n(L_v)) \to H^1(S_n, M_n)^* \quad (15)$$

where the sum is taken over all places v and where $S_{n,v}$ is the decomposition group at vlace v. As the first Tate-Shafarevic group is finite for every torus and as $H^1(S_n, M_n)$ is finite, the result will follow if we can prove that $\oplus H^1(S_{n,v}, T_n(L_v))$ is infinite. By local duality we know that $H^1(S_{n,v}, T_n(L_v)) \simeq H^1(S_{n,v}, M_n)^*$. By Tchebotarev's density theorem (e.g. [6,p.132]) we know that there are infinitely many places v s.t. $S_{n,v}$ is conjugated to the cyclic subgroup C generated by the permutation $(1...m)(m+1...n)$ where $n = m.k$ is a nontrivial factorization of n. Using the defining sequence of M_n and using duality for cyclic groups it is then easy to verify that

$$H^1(C, M_n) \simeq \mathbb{Z}/m\mathbb{Z} \quad (16)$$

finishing the proof. □

References

[1] Chr. Bessenrodt,L. Le Bruyn : "Stable rationality of certain PGL_n- quotients" to appear

[2] J.L. Brylinski : "Décomposition simpliciale d'un réseau, invariante par un groupe fini d'automorphismes" C.R.Acad.Sc.Paris 288 (1979) 137-139

[3] J.L. Colliot-Thélène,J.J. Sansuc : "La R-équivalence sur les tores" Ann.Scient.E.N.S. 10 (1977) 175-230

[4] J.L. Colliot-Thélène : "L'équivalence rationnelle sur les tores"Sém. Théorie des Nombres de Bordeaux 1975/76,exp. 15

[5] Yu. Manin : "Cubic forms : algebra,geometry,arithmetic" North-Holland (1974)

[6] J. Neukirch : "Class field theory" Springer-Verlag (1986)

[7] V.E. Voskresenskii : "Algebraicheskie tory",Nauka (1977)

[8] J.L. Colliot-Thélène,J.J. Sansuc : "Principal homogenous spaces under flasque tori,applications" J.Alg. 106 (1987) 148-205