Generic Norm One Tori

Lieven Le Bruyn
Research Associate NFWO (Belgium)

Department of Mathematics & Computer Science
University of Antwerp, UIA, Belgium

October 1994 Report no. 94-22

Dedicated to Prof. W. Kuijk

Division of Pure Mathematics
Department of Mathematics & Computer Science

universitaire instelling antwerpen

Universiteitsplein 1, B-2610 Wilrijk-Antwerpen , BELGIUM

Generic Norm One Tori

Lieven Le Bruyn
Research Associate NFWO (Belgium)

Department of Mathematics & Computer Science
University of Antwerp, UIA, Belgium

October 1994 Report no. 94-22

Dedicated to Prof. W. Kuijk

Key Words and Phrases
Lattice- and Tori-Invariants, Rationality Questions, Galois Theory, Noether Problem

GENERIC NORM ONE TORI

LIEVEN LE BRUYN

Dedicated to Prof. W. Kuyk

1. Introduction

Much of the early work of Prof. W. Kuyk [8, 9] deals with Noether's problem in Galois theory, that is, whether every finite group G can be realized as a Galois group over a given number field k and if so, can all Galois extensions with group G be parametrized in a simple way. E. Noether showed in [13] that both questions have an affirmative answer if one can prove that $k(x_1, ..., x_n)^G$ is a purely trancendental field extension of k whenever G acts faithfully by permutations on a finite set of indeterminates $x_1, ..., x_n$. Apart from eliminating some exceptions in Noether's handling of the problem, the results of W. Kuyk (e.g. what we now know as 'Kuyk's lemma' [16, Lemma 4.5]) paved the way for D. Saltman's [14] formulation of the Noether problem in terms of 'generic Galois extensions'. For a survey of the Noether problem as well as W. Kuyk's contribution we refer the reader to the excellent papers by R.G. Swan [16, 17].

Counterexamples to the rationality version of Noether's problem over $k = \mathbb{Q}$ were given by R.G. Swan [18] and V.E. Voskresenskii [19]. A full solution to the rationality problem for an Abelian group was given by H.W. Lenstra in [11] and the remaining problem whether rationality holds for $k = \mathbb{C}$ was finally settled in the negative by D. Saltman [15]. Crucial to all these papers are results on lattice- and tori-invariants.

My own interest in Noether's problem and related questions on tori-invariants resulted from the (stable) rationality problem of m-tuples of $n \times n$ matrices under simultaneous conjugation by $PGL_n(\mathbb{C})$. Work of C. Procesi and E. Formanek [6] reduces this problem to the (stable) rationality of a certain field of tori-invariants. E. Formanek [6, 7] succeeded in proving rationality of these tori-invariants for $n = 3$ and $n = 4$. Using results of J.L. Colliot-Thélène and J.J. Sansuc [4] and modular representation theory of the symmetric group, Ch. Bessenrodt and myself were able to prove stable rationality of the quotient variety $M_n(\mathbb{C})^{\oplus m}/PGL_n$ for all n dividing 420, [1]. For an account of the history and applications of this problem we refer the reader to [10].

Key words and phrases. Lattice- and tori-invariants, rationality questions, Galois theory, Noether problem.

Research associate NFWO (Belgium)

Afterwards, it became clear that our results can also be phrased in Galois theory, in particular the parametrization of norm one elements in generic degree n field extensions. This special volume dedicated to Prof. W. Kuyk seems to be an excellent opportunity to explain some of these connections.

2. Summary of the results

In this note we aim to study the norm-one torus $R^1_{K/k}\mathbb{G}_m$ for a finite separable field extension 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's theorem 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 the Galois group $Gal(K/k)$.

If K/k is Galois but no longer (meta)cyclic, finding parametrizations of all k-rational points of the norm one torus $R^1_{K/k}\mathbb{G}_m$ usually is a rather hopeless task as the following example due to J.L. Colliot-Thélène and J.J. Sansuc [4, 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 [4] or [12].

The situation becomes even more complicated in case K/k is no longer Galois, see [4, p.209-212] for some of the rare manageable cases. In this note we will study the generic case, that is, K/k is separable of degree n such that the Galois closure L has Galois group S_n. Some of the results hold for arbitrary degree n extensions using restriction from S_n to the Galois group of the extension but we will leave the details to the interested reader.

Let us give an easy example of the situation of interest to us : take $K = \mathbb{Q}(\sqrt[3]{2})$ over $\mathbb{Q}$, then the Galois closure of K is $L = \mathbb{Q}(\sqrt[3]{2}, i\sqrt{3})$ and $Gal(L/\mathbb{Q}) = S_3$. In this case, $R^1_{K/\mathbb{Q}}\mathbb{G}_m$ is determined by the equation

$$x^3 + 2y^3 + 4z^3 - 6xyz = 1$$

and we want to find all the $\mathbb{Q}$-rational points on this surface. As S_3 is a dihedral group we can apply [3, II.1.c] and obtain that $R^1_{K/\mathbb{Q}}\mathbb{G}_m$ is a $\mathbb{Q}$-rational variety and 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. Clearly, this approach can no longer be used for generic field extensions of degree $n > 3$.

Indeed, we will show that the situation becomes more complicated if n increases : the generic norm one torus $R^1_{K/k}\mathbb{G}_m$ is no longer k-rational if $n = [K : k] \geq 4$ (at least for prime and non-squarefree values of n). Still, for prime degree extensions we will show that it is possible to determine all k-rational points of $R^1_{K/k}\mathbb{G}_m$ by a Hilbert-like procedure, that is, 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 and proofs are dual to those of [1] we will merely sketch the main ideas and refer the reader to loc.cit. for more details.

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

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

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

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 such that $N_{K/k}(x) \neq 0$.

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 $G = Gal(L/k)$. This correspondence is 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 $\mathbb{Z}$ and $R_{K/k}\,\mathbb{G}_m$ to the permutation lattice $\mathbb{Z}G/H$ where H is the subgroup of G such that $L^H = K$. $R^1_{K/k}\mathbb{G}_m$ corresponds to $J_{G/H}$ which is determined by the exact sequence of $\mathbb{Z}G$ lattices

$$0 \to \mathbb{Z} \to \mathbb{Z}G/H \to J_{G/H} \to 0$$

the first map being the norm map $1 \to \sum gH$.

J.L. Brylinski [2] obtained an algorithmic procedure to construct a smooth proper equivariant k-model X_T for a given algebraic k-torus T. The embedding $T \hookrightarrow X_T$ gives rise to an exact sequence of $\mathbb{Z}G$-lattices

$$0 \to \hat{T} \to Div_{Y \times_k K}(X_T \times_k K) \to Pic(X_T \times_k K) \to 0$$

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 proved in [20] that if the torus T is k-rational then the $\mathbb{Z}G$-lattice $Pic(X_T \times_k K)$ has to be a stable permutation $\mathbb{Z}G$- lattice, meaning that there exist permutation lattices P_1 and P_2 such that

$$Pic(X_T \times_k K) \oplus P_1 \simeq P_2$$

We are now in a position to state and prove :

Theorem 3.1. If K/k is a finite separable field extension 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

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

where the left hand map is induced from $\mathbb{Z}S_p/S_{p-1} \to \mathbb{Z}S_p/S_{p-2}$ sending x_i to $\sum_j (y_{ij} - y_{ji})$ where the x_i (resp y_{ij}) are the canonical base vectors 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 (that is, 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

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

where $\mathbb{P}$ is a projective $\mathbb{Z}G$-module (hence invertible) and because the Sylow p-subgroup of S_p is cyclic $\Omega^{-2}(\hat{\mathbb{Z}}_p)$ is also invertible, proving our claim (using duality and Shapiro's lemma).

Now, using flasqueness of M_p and $Pic(X \times_k K)$ one easily verifies that

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

Therefore, we have to show that M_p cannot be a stable permutation lattice. 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-hypo elementary subgroup $N_p = N_{S_p}(Syl_p(S_p))$) which enables us to show that

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

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

A cohomological argument due to R. Snider and D. Saltman shows that a similar statement also holds for all non-squarefree degrees n. The remaining case of squarefree but composite degrees is open. I conjecture that the norm one torus $R^1_{K/k}\mathbb{G}_m$ will never be a k-rational variety if the degree of K/k is ≥ 4 with 6 as the only possible exception.

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

The foregoing result may suggest that it will be rather hard to find an explicit Hilbert-like parametrization of all k-rational points on the norm one torus $R^1_{K/k}\mathbb{G}_m$. However, a result of J.L. Colliot-Thélène and J.J. Sansuc [5, Prop.9.1] offers some hope. They show that $Pic(X \times_k K)$ is a direct factor of a permutation lattice. Exactly as in the proof of the following theorem this shows that a Hilbert-like parametrization of the norm one elements is in principle possible. However, their general argument gives a middle term permutation lattice which is much too large to be of any practical value.

It is precisely in this respect that the next result improves dramatically on the Colliot-Thélène and Sansuc theorem.

Theorem 4.1. Let K/k be a separable field extension of prime degree p with Galois closure L with group S_p. Then, all k- rational points on $R^1_{K/k}\mathbb{G}_m$ (alternatively, all norm one elements of K^*) can be written as

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

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

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

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

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

where $\mathcal{G}$ is the absolute Galois group $Gal(k_s/k)$.

Now, for any field extension $k \subset M \subset k_s$ 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's theorem 90. So, the last term vanishes. Also the next to last term vanishes as we have a torus U_p such that

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

for some intermediate fields $k \subset K_i \subset L$.

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

5. The global case

For any degree n extension K/k, elements of K of the form $N_{K'/K}(\frac{\alpha}{(12).\alpha})$ clearly have norm one. However, if n is composite there may be others. We will now show that the image in this case is not even of finite index, if k is a number (or global) field.

Theorem 5.1. Let K/k be a finite separable field extension of degree n of numberfields, such that the Galois closure L has group S_n. If n is composite, then the cokernel of the map

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

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

Proof. The Tate-Nakayama exact sequence gives us the following exact sequence

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

where the sum is taken over all places v and where $S_{n,v}$ is the decomposition group at place v.

Because the first Tate-Shafarevic group Ш^1 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 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

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

finishing the proof. □

References

1. Ch. Bessenrodt, L. Le Bruyn : Stable rationality of certain PGL_n-quotients, Invent. Math. 104 (1991) 179-199
2. J.L. Brylinski : Décomposition simpliciale d'un reseau, invariante par un groupe fini d'automorphismes, C.R. Acad. Sci. Paris 288 (1979) 137-139
3. J.L. Colliot-Thelene : L'équivalence rationnelle sur les tores, Séminaire de théorie des nombres de Bordeaux, Année 1975-76 exposé 15 (1976)
4. J.L. Colliot-Thelene, J.J. Sansuc : La R-equivalence sur les tores, Ann. Sci. ENS 10 (1977) 175-229
5. J.L. Colliot-Thelene, J.J. Sansuc : Principal homogeneous spaces under flasque tori : applications, J. Alg. 106 (1987) 148-205
6. E. Formanek : The center of the ring of 3×3 generic matrices, Lin. Mult. Alg. 7 (1979) 203-212
7. E. Formanek : The center of the ring of 4×4 generic matrices, J. Alg. 62 (1980) 304-319
8. W. Kuyk : Over het omkeerprobleem van de Galoistheorie, Thesis, Amsterdam 1960

9. W. Kuyk : On a theorem of E. Noether, Nederl. Akad. Wetensch. Proc. Ser. A 67 (1964) 32-39
10. L. Le Bruyn : Centers of generic division algebras, the rationality problem 1965-90, Israel J. Math. 76 (1991) 97-111
11. H.W. Lenstra : Rational functions invariant under a finite Abelian group, Invent. Math. 25 (1974) 299-325
12. Y.I. Manin : "Cubic forms, algebra, geometry, arithmetic" monograph North-Holland Publ. (1974)
13. E. Noether : Gleichungen mit vorgeschriebener Gruppe, Math. Ann. 78 (1918) 221-229
14. D. Saltman : Generic Galois extensions and problems in field theory, Adv. Math. 43 (1982) 250-283
15. D. Saltman : Noether's problem over an algebraically closed field, Invent. Math. 77 (1984) 71-84
16. R.G. Swan : Noether's problem in Galois theory, in "Emmy Noether in Bryn Mawr" ed. B. Srinivasan and J. Sally, Springer (1983) 21-40
17. R.G. Swan : Galois theory, in "Emmy Noether, a tribute to her life and work" ed. J.W. Brewer and M.K. Smith, Marcel Dekker (1981) 115-124
18. R.G. Swan : Invariant rational functions and a problem of Steenrod, Invent. Math. 7 (1969) 148-158
19. V.E. Voskresenskii : On the question of the structure of the subfield of invariants of a cyclic group of automorphisms of the field $\mathbb{Q}(x_1, ..., x_n)$, Math. USSR-Izv. 5 (1970) 371-380
20. V.E. Voskresenskii : "Algebraicheskie tory" (in Russian) Nauka (1977)

UNIVERSITAIRE INSTELLING ANTWERPEN, B-2610 WILRIJK, BELGIUM
E-mail address: lebruyn@wins.uia.ac.be