

SPLITTING FIELDS OF CHARACTERISTIC POLYNOMIALS IN ALGEBRAIC GROUPS

E. KOWALSKI

In [K1] and earlier in [K2], questions of the following type are considered: suppose a family $(g_i)_i$ of matrices in some (algebraic) matrix group are given, with rational coefficients. What is the “typical” Galois group of the splitting field K_i of the characteristic polynomial of g_i (defined as the field generated over \mathbf{Q} by the roots of the characteristic polynomial)? Is this characteristic polynomial typically irreducible? If the elements g_i are in $GL(n, \mathbf{Q})$, or in $SL(n, \mathbf{Q})$, there is an obvious “upper bound”, namely the symmetric group \mathfrak{S}_n . If the elements g_i are in a symplectic group (for an alternating form with rational coefficients), or in the group of symplectic similitude, there is also an easy, if slightly less obvious, upper bound: the characteristic polynomial satisfies some relation such as

$$T^{2g}P(T^{-1}) = P(T)$$

if $g_i \in Sp(2g, \mathbf{Q})$ for instance, and this leads to relations among the roots which are easily shown to imply that the Galois group of the splitting field is, as subgroup of \mathfrak{S}_{2g} , isomorphic to a subgroup of W_{2g} , defined as the group of permutations of the g pairs $(2i - 1, 2i)$, $1 \leq i \leq g$, which also permute the pairs.

Now, intrinsically, W_{2g} is also the Weyl group of the algebraic group $Sp(2g)$, or of $CSp(2g)$, just as \mathfrak{S}_n is the Weyl group of $GL(n)$ or $SL(n)$. It is natural to believe that this is not a coincidence, and then to go on to expect a more general result along these lines; also, it seems reasonable to look for a better explanation than that above, even for those easy cases.

In this note, we consider this question and get an “intrinsic” result, though not yet in the most general case.

Let G/K be a reductive (connected) linear algebraic group over a field K , which we assume to be perfect. We assume G is given as a subgroup of $GL(n)$ for some n , and that the intersection

$$T = G \cap T_n,$$

where T_n is the group of diagonal matrices in $GL(n)$, is a maximal torus of G .

Let now $g \in G(K)$ be given. We are interested in the splitting field of the characteristic polynomial $\det(T - g)$, defined and computed when seeing g as a matrix in $GL(n, K)$.

Let $g = g_s g_u$ be the Jordan decomposition of g . Define

$$X_g = \{t \in T \mid t \text{ and } g_s \text{ are conjugate.}\}$$

Note that $X_g \neq \emptyset$ because any semisimple element (here, g_s) lies in some maximal torus, and any maximal torus is conjugate to T . Moreover, note that the normalizer $N(T)$ of T acts on X_g by conjugation, and that $T \subset N(T)$ (which is also the centralizer of T because G is reductive) acts trivially, so that the Weyl group $W(G) = N(T)/T$ acts naturally on X_g .

Now we have the following two lemmas:

Lemma 1. *The splitting field K_g of $\det(T - g)$ is the field $K(t_0)$ generated by the coordinates of any $t_0 \in X_g$.*

Proof. If (t_1, \dots, t_n) are the diagonal coefficients of $t_0 \in X_g$, then we have

$$\det(T - g) = \det(T - g_s) = \det(T - t_0) = \prod_{i=1}^n (T - t_i)$$

so that the roots of $\det(T - g)$ are simply the coordinates of t_0 , hence the result. \square

Lemma 2. (1) *The action of $W(G)$ on X_g is transitive.*

(2) *Let $t_0 \in X_g$ be given. If $C(t_0) \cap N(G) = T$, where $C(t_0)$ is the centralizer of t_0 in G , then the action of $W(G)$ on X_g is free. In particular, this is true if $C(g_s)$ is a maximal torus.*

Proof. We may assume that $g = g_s$ is semisimple for both statements.

(1) Fix $t_0 \in X_g$ as in (2). For any $t \in X_g$, by definition t and t_0 are conjugate in G . However it is known that if two elements of a maximal torus of a connected linear algebraic group are conjugate, then they are conjugate under the normalizer of the maximal torus (see, e.g., [DM, Cor. 0.12, (iv)]). Here this means there exists $w \in N(T)$ with $w \cdot t = t_0$.

(2) If $w \in N(T)$ is such that $w \cdot t_0 = t_0$, we have $w \in N(T) \cap C(t_0) = T$ by assumption. Hence w is trivial in $W(G)$.

For the last statement, if $C(g_s)$ is a maximal torus, then so is $C(t_0)$, and since it contains T , it must be equal to T , hence the result. \square

Putting together both lemmas, we see that if $g \in G(K)$ has the property that $C(g_s)$ is a maximal torus, then we can define a map

$$\begin{cases} \text{Gal}(\bar{K}/K) \rightarrow W(G) \\ \sigma \mapsto w_\sigma \end{cases}$$

where w_σ is the unique element of $W(G)$ such that

$$\sigma(t_0) = w_\sigma^{-1} \cdot t_0$$

(again, $t_0 \in X_g$ is fixed). Here we use that $\sigma(t_0) \in X_g$ because $g \in G(K)$.

Since it is also a fact that representatives \dot{w} of $w \in W(G)$ in $N(T)$ can be chosen in $G(K)$ (see, e.g., [Sp, Par. before 16.1.3]), it is easy to deduce that the map above is in fact a group homomorphism:

$$(\sigma\tau)(t_0) = \sigma(w_\tau^{-1} \cdot t_0) = \sigma(\dot{w}_\tau^{-1} t_0 \dot{w}_\tau) = \dot{w}_\tau^{-1} \sigma(t_0) \dot{w}_\tau = w_\tau^{-1} \cdot w_\sigma^{-1} \cdot t_0 = w_{\sigma\tau}^{-1} \cdot t_0$$

so $w_{\sigma\tau} = w_\sigma w_\tau$.

Moreover, the kernel of this group homomorphism is by definition the group of $\sigma \in \text{Gal}(\bar{K}/K)$ such that $\sigma(t_0) = t_0$, hence it is the field generated by coefficients of t_0 , i.e., by the first lemma, it is the splitting field of $\det(T - g)$. In other words, under the assumption that $C(g_s)$ is a maximal torus, we have an injective homomorphism

$$\text{Gal}(K_g/K) \rightarrow W(G).$$

Proposition 3. *Let G be a connected reductive group which is a product of groups of type $GL(n)$, $SL(n)$, $Sp(2g)$, $CSp(2g)$, embedded in $GL(r)$ for the obvious r in the obvious way, or more generally, assume that $G \subset GL(n)$ is simply-connected, in addition to the assumptions*

at the beginning of the note. Let $g \in G(K)$ be a regular semisimple element. Then there is an injective homomorphism

$$\mathrm{Gal}(K_g/K) \rightarrow W(G).$$

Proof. The only thing to remember is first that if g is a regular semisimple element in a connected reductive group, then the connected component $C(g)^0$ of $C(g)$ is a maximal torus (see, e.g., [Bo, II.12.2, Prop.]), and second that if G is simply-connected, then the centralizer of a semisimple element is connected (a result of Steinberg; see, e.g., [St, Th. 2.15] or [Ca, Th. 3.5.6]). Together with the previous results, the statement follows. \square

The restriction to regular elements can be bypassed by specialization: working with the field $L = K(G)$, the function field of G . The generic element $\eta \in G(L)$ is obviously regular, and thus we derive an injection

$$\mathrm{Gal}(L_\eta/L) \rightarrow W(G)$$

where L_η is the splitting field of the characteristic polynomial $P_\eta = \det(T - \eta)$ of η (which is in $L[T]$). Any $g \in G(K)$ is a specialization of η and its characteristic polynomial is a specialization of P_η ; thus the Galois group of its splitting field is isomorphic to a subgroup of W .

In fact, it seems likely that $\mathrm{Gal}(L_\eta/L)$ is isomorphic to $W(G)$ in the situations above. This is certainly the case for $K = \mathbf{Q}$.

Note also that Corvaja [Co, Cor. 1.11] has proved general results showing that this “generic” Galois group is always “attained” by some rational element $g \in G(K)$ if $G(K)$ is Zariski-dense in G and K is finitely generated.

Remark 4. The condition of simple-connectedness above is not merely technical. Indeed, consider $G = PSL(2)/\mathbf{Q}(i)$ and the class of the matrix

$$g = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}$$

which is a regular element of $G(\mathbf{Q}(i))$. The centralizer of g in G is the union of the matrices of the two types

$$\begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix}, \quad \begin{pmatrix} 0 & -a \\ a^{-1} & 0 \end{pmatrix}$$

so it is of dimension 1 but not connected.¹ It is the normalizer of the diagonal maximal torus of $PSL(2)$, so that the second component represents the non-trivial element of the Weyl group. The defining field of g is $\mathbf{Q}(i)$, but to speak of characteristic polynomial we must use a faithful representation, the simplest of which is the symmetric square $PSL(2) \rightarrow GL(3)$,² which maps

$$g \mapsto \begin{pmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{pmatrix}$$

and there the characteristic polynomial has trivial splitting field.

¹ This is one of the simplest examples of this phenomenon for a connected group.

² Which can be seen as the action of $PSL(2)$ on quadratic polynomials $aX^2 + bXY + cY^2$ induced by unimodular linear substitutions, i.e., by $SL(2)$.

Remark 5. There is an alternate construction (which is maybe better; it appears for different purposes in the theory of character sheaves, see the beginning of Laumon’s Bourbaki report on Lusztig’s work), where instead of X_g one looks at

$$Y_g = \{y \in G/T \mid y g_s y^{-1} \in T\},$$

(i.e., the “conjugators” to T instead of the conjugates in T) and then under the assumptions that G is connected reductive and g is regular semisimple, one checks that Y_g is a principal homogeneous space under $W(G)$, under the action $w \cdot y = yw$. This leads to a homomorphism

$$\mathrm{Gal}(\bar{K}/K) \rightarrow W(G)$$

by $\sigma \mapsto w_\sigma$, where $\sigma(y_0) = w \cdot y_0$ for a fixed $y_0 \in Y_g$. Now simple-connectedness (or similar) assumptions arise when showing that the kernel of this map is the Galois group $\mathrm{Gal}(\bar{K}/K_g)$, where K_g is the splitting field of $\det(T - g)$.

Remark 6. In some applications, we have a $g \in G(K)$ such that $\det(T - g) \in k[T]$ for some subfield $k \subset K$. In that case, it is of course more interesting to know the Galois group of the splitting field of $\det(T - g)$ as an extension of k instead of K . For instance, this arises when looking at Frobenius elements (conjugacy classes really) in algebraic geometry, with (typically) $K = \mathbf{Q}_\ell$ for some prime ℓ and $k = \mathbf{Q}$. This may still be dealt with using the arguments above, if the following conditions are true: (1) G is obtained by base change from a group \tilde{G} defined over k ; (2) representatives of $W(G)$ in $N(T)$ can be found obtained by base change from representatives of $W(\tilde{G})$; (3) two elements in $G(K)$ with the same characteristic polynomial are conjugate.

Indeed, under such assumptions, note that Lemma 1 holds for the splitting field k_g over k and the field $k(t_0)$ generated over k by the eigenvalues, since the characteristic polynomial has coefficients in k ; Lemma 2 holds unchanged; and the definition of the map

$$\begin{cases} \mathrm{Gal}(\bar{k}/k) \rightarrow W(G) \\ \sigma \mapsto w_\sigma \text{ such that } \sigma(t_0) = w_\sigma \cdot t_0 \end{cases}$$

is valid, because $\sigma(t_0) \in X_g$ still holds (although $g \notin G(K)$ a priori), since it has characteristic polynomial equal to $\det(T - t_0)^\sigma = \det(T - t_0)$, and we can use assumption (3). Then Assumptions (1) and (2) imply that this remains a homomorphism.

The conditions (1), (2) are clearly true for most (if not all?) reductive groups in characteristic zero at least. Condition (3) holds for $GL(n)$ and $CSp(2g)$, at least.

Note, however, that this argument is not easily amenable to specialization to deal with elements with g_s non-regular.

REFERENCES

- [Bo] A. Borel: *Linear algebraic groups*, 2nd edition, GTM 126, Springer 1991.
- [Ca] R.W. Carter: *Finite groups of Lie type*, Wiley Interscience 1985.
- [Co] P. Corvaja: *Rational fixed points for linear group actions*, preprint (2006), [arXiv:math/0610661v2](https://arxiv.org/abs/math/0610661v2).
- [DM] F. Digne and J. Michel: *Representations of finite groups of Lie type*, L.M.S Student Texts 21, Cambridge University Press 1991.
- [K1] E. Kowalski: *The large sieve and its applications: arithmetic geometry, random walks, discrete groups*, Cambridge Univ. Tracts (to appear).
- [K2] E. Kowalski: *The large sieve, monodromy and zeta functions of curves*, J. reine angew. Math 601 (2006), 29–69.

- [Sp] T.A. Springer: *Linear algebraic groups*, 2nd edition, Progr. Math. 9, Birkhäuser 1998.
[St] R. Steinberg: *Torsion in reductive groups*, Advances in Math. 15 (1975), 63–92.

UNIVERSITÉ BORDEAUX I - A2X, 351, COURS DE LA LIBÉRATION, 33405 TALENCE CEDEX, FRANCE
E-mail address: `emmanuel.kowalski@math.u-bordeaux1.fr`