HERMITE’S THEOREM VIA GALOIS COHOMOLOGY

MATTHEW BRASSIL AND ZINOVY REICHSTEIN

Abstract. An 1861 theorem of Hermite asserts that for every field extension $E/F$ of degree 5 there exists an element of $E$ whose minimal polynomial over $F$ is of the form $f(x) = x^5 + c_2 x^3 + c_4 x + c_5$ for some $c_2, c_4, c_5 \in F$. We give a new proof of this theorem using techniques of Galois cohomology, under a mild assumption on $F$.

1. Introduction

An 1861 theorem of Hermite asserts that for every field extension $E/F$ of degree 5 there exists an element of $E$ whose minimal polynomial over $F$ is of the form $f(x) = x^5 + c_2 x^3 + c_4 x + c_5$ for some $c_2, c_4, c_5 \in F$.

Modern proofs of this result have been given by Coray [8] and Kraft [12]. Coray’s proof relies on techniques of arithmetic geometry, whereas Kraft’s is based on representation theory, in the spirit of Hermite’s original paper [9]. The purpose of this note is to give yet another proof of the following variant of Hermite’s theorem using techniques of Galois cohomology.

Theorem 1. Let $E/F$ be a field extension of degree 5. Assume $F$ contains an algebraically closed field $k$. Then there exists an element $a \in E$ whose minimal polynomial is of the form $f(x) = x^5 + c_2 x^3 + c_4 x + c_5$ for some $c_2, c_4, c_5 \in F$.

2. A geometric restatement of the problem

Clearly every $z \in E \setminus F$ is a primitive element for $E/F$. Choose one such $z$ and set $a = x_0 + x_1 z + \cdots + x_4 z^4 \in E$, where $x_0, \ldots, x_4 \in F$ are to be specified later. The characteristic polynomial of $a$ over $F$ is $f(t) = \det(t \cdot 1_F - a) = t^5 + c_1 t^4 + \cdots + c_4 t + c_5$, where $t$ is a commuting variable, and $\det$ denotes the norm in the field extension $E(t)/F(t)$. Each $c_i$ is a homogeneous polynomial of degree $i$ in $x_0, \ldots, x_4$ with coefficients in $F$. We are interested in non-trivial solutions of the system

$$c_1(x_0, \ldots, x_4) = c_3(x_0, \ldots, x_4) = 0$$

in $\mathbb{P}^4(F)$. Note that $c_1$ cuts out a linear subvariety $\mathbb{P}^3 \subset \mathbb{P}^4$, and $c_3$ cuts out a cubic surface in this $\mathbb{P}^3$ defined over $F$. We will denote this cubic surface by $X$. Any solution $(x_0 : \ldots : x_4) \in \mathbb{P}^4(F)$ to (1) (or equivalently, any $F$-point of $X$) gives rise to an element $a = x_0 + x_1 z + \cdots + x_4 z^4 \in E$ whose characteristic polynomial is of the desired form. Moreover, if $(x_0 : \ldots : x_4) \neq (1 : 0 : \ldots : 0)$, then $a$ is a primitive element of $E$, so its minimal polynomial is the same as its characteristic polynomial.

2010 Mathematics Subject Classification. 12G05, 14G05.

Key words and phrases. Hermite's theorem, quintic polynomial, Galois cohomology, Tsen-Lang theorem, essential dimension.

Zinovy Reichstein was partially supported by National Sciences and Engineering Research Council of Canada Discovery grant 253424-2017.
Lemma 2. (a) $(1 : 0 : 0 : 0 : 0)$ is a solution to (1) if and only if $\text{char}(F) = 5$.

(b) In the course of proving Theorem 1, we may assume without loss of generality that $\text{char}(F) \neq 5$. In particular, we may assume that $E/F$ is separable.

(c) In order to prove Theorem 1, it suffices to show that the system (1) has a non-trivial solution in $F$ (or equivalently, $X$ has an $F$-point).

Proof. (a) If $x_0 = 1$ and $x_1 = \cdots = x_4 = 0$, then $a = 1$, and
\[
\det(t \cdot 1_F - a) = (t - 1)^5 = t^5 - 5t^4 + 10t^3 - 10t^2 + 5t - 1,
\]
so $c_1 = -5$ and $c_3 = -10$. Thus $c_1 = c_3 = 0$ if and only if $\text{char}(F) = 5$.

(b) An easy application of the Jacobian criterion, shows that the surface $X$ is smooth whenever $\text{char}(k) \neq 3$; see [8, Lemma 1.2].

Assume $\text{char}(F) = 5$. By part (a), $(1 : 0 : \cdots : 0)$ is an $F$-point of $X$. Consequently, by [11, Theorem 1.1], $X$ is unirational over $F$. Since $F$ is an infinite field (recall that we are assuming that $F$ contains an algebraically closed field), this tells us that $F$-points are dense in $X$. In particular, there is an $F$-point on $X$, other than $(1 : 0 : 0 : 0 : 0)$, as desired.

(c) By part (b), we may assume that $\text{char}(k) \neq 5$. By part (a), $(1 : 0 : 0 : 0 : 0)$ is not a solution to (1). Thus any solution gives rise to $a = x_0 + x_1z + \ldots + x_4z^4 \in E$ whose minimal polynomial has the desired form. $\square$

3. Preliminaries on Galois cohomology and essential dimension

In this section we give a brief summary of the background material on Galois cohomology and essential dimension, which will be used in the sequel. For details we refer the reader to [17, 18, Chapter I], [5], and [15].

- Let $G$ be a smooth algebraic group over $k$ and $F$ be a field. The Galois cohomology set $H^1(F, G)$ is in a natural bijective correspondence with isomorphism classes of $G$-torsors $T \to \text{Spec}(F)$. The class of the split torsor $G \times_{\text{Spec}(k)} \text{Spec}(F) \to \text{Spec}(F)$ is usually denoted by $1 \in H^1(F, G)$.

- In the case where $G$ is the symmetric group $S_n$ (viewed as a constant finite group over $k$), the Galois cohomology set $H^1(F, S_n)$ is also in a natural bijective correspondence with isomorphism classes of $n$-dimensional étale algebras $E/F$. Recall that an étale algebra $E$ is, by definition, is a direct product of the form $E = E_1 \times \ldots \times E_r$, where each $E_i/F$ is a finite separable field extension.

- In particular, a separable field extension $E/F$ of degree $n$ gives rise to a class in $H^1(F, S_n)$. This class lies in the image of the natural map $H^1(F, G) \to H^1(F, S_n)$, for a subgroup $G$ of $S_n$ if and only if the Galois group of $E/F$ is contained in $G$.

- Let $E/F$ be a finite field extension, and $k \subset F$ be a subfield. We say that $E/F$ descends to an intermediate extension $k \subset F_0 \subset F$ if $E = E_0 \otimes_{F_0} F$ for some field extension $E_0/F_0$. The essential dimension $\text{ed}(E/F)$ is the minimal transcendence degree $\text{trdeg}_k(F_0)$ such that $E/F$ descends to $F_0$. This number depends on the base field $k$, which we assume to be fixed throughout.

- If $G$ is an algebraic group over $k$, then the essential dimension $\text{ed}(\tau)$ of a $G$-torsor $\tau : T \to \text{Spec}(F)$ is defined in a similar manner. We say that $\tau$ descends to a subfield $F_0 \subset F$ if it lies in the image of the natural map $H^1(F_0, G) \to H^1(F, G)$. The essential dimension $\text{ed}(\tau)$ is the minimal transcendence degree of
structible extension

non-trivial finite field extension $E/F$

both parts of Lemma 3 and in Proposition 5.

Remark 6

Proof. (a) By [8, Proposition 2.2], our cubic surface $X$ follows from (a).

towers of quadratic field extensions appear naturally; see, e.g., [1, Section 13.4].

Let $\text{Lemma 4}.$

has an $E/F$ separable field extension $E/F$

apply (a) recursively. However, in view of Lemma 4, it suffices to prove the following.

Proposition 5.

For every separable field extension $E/F$ of degree 5, there exists a constructible extension $F'/F$ such that $\text{ed}(E'/F') \leq 1$. Here $E' = E \otimes_F F'$.

Remark 6. Since $k$ is algebraically closed, it is easy to see that $\text{ed}(E/F) \geq 1$ for every non-trivial finite field extension $E/F$ (with $E \neq F$). Thus $\leq 1$ can be replaced by $= 1$ in both parts of Lemma 3 and in Proposition 5.

The term “constructible” is related to the classical theory of ruler and compass constructions, where towers of quadratic field extensions appear naturally; see, e.g., [1] Section 13.4.
5. Conclusion of the proof of the main theorem

In this section we will complete the proof of Theorem 1 by establishing Proposition 5. Let \( \alpha \) denote the class of the field extension \( E/F \) in \( H^1(F, S_5) \). Consider the exact sequence

\[
1 \rightarrow A_5 \rightarrow S_5 \xrightarrow{\text{sign}} \mathbb{Z}/2\mathbb{Z} \rightarrow 1,
\]
and the associated sequence

\[
H^1(F, A_5) \rightarrow H^1(F, S_5) \xrightarrow{D} H^1(F, \mathbb{Z}/2\mathbb{Z})
\]

of Galois cohomology sets; cf. [17, Section 5.5]. Here, as usual, \( A_5 \) denotes the alternating subgroup of \( S_5 \). (If \( \text{char}(F) \neq 2 \), \( D(\alpha) \) is just the discriminant of \( E/F \), viewed as an element of \( H^1(F, \mathbb{Z}/2\mathbb{Z}) \).)

Note that this reduction does not, by itself, allow us to conclude that \( \text{ed}(E/F) \leq 1 \). Indeed, \( \text{ed}(A_5) = 2 \), assuming \( \text{char}(k) \neq 2 \); see [2, Theorem 6.7]. We will need to pass to a further constructible extension \( F'/F \) in order to ensure that \( \text{ed}(E/F) \leq 1 \).

For notational simplicity, we will continue to denote the class of \( E/F \) in \( H^1(F, A_5) \) by \( \alpha \). Since \( k \) is algebraically closed, \( A_5 \) can be embedded in \( \text{PGL}_2(k) \); see [16, p.19-04].

Let us now consider the commutative diagram

\[
\begin{array}{cccccc}
1 & \rightarrow & G_m & \rightarrow & \text{GL}_2 & \rightarrow & \text{PGL}_2 & \rightarrow & 1 \\
1 & \rightarrow & G_m & \rightarrow & G & \rightarrow & A_5 & \rightarrow & 1 \\
\end{array}
\]

of algebraic groups over \( k \), where \( G \) is the preimage of \( A_5 \) in \( \text{GL}_2 \). This diagram induces a commutative diagram

\[
\begin{array}{ccc}
H^1(F, \text{PGL}_2) & \xrightarrow{\delta} & H^2(F, G_m) \\
\downarrow & & \downarrow \\
H^1(F, G) & \xrightarrow{\pi_F} & H^1(F, A_5) & \xrightarrow{\delta} & H^2(F, G_m) \\
\end{array}
\]

of Galois cohomology sets, where the bottom row is exact; cf. [17, Section 5.5]. Here \( \delta \) denotes the connecting map. The class of \( \delta(\alpha) \) is represented by a quaternion algebra over \( F \). This algebra can be split by a quadratic extension \( F'/F \). After replacing \( F \) by \( F' \), we may assume that \( \delta(\alpha) = 0 \). Equivalently, \( \alpha = \pi_F(\beta) \) for some \( \beta \in H^1(F, G) \).

Since \( \dim(G) = 1 \) and the natural 2-dimensional representation of \( G \) is generically free (i.e., the stabilizer of a general point in trivial), one readily concludes that \( \text{ed}(G) = 1 \); see [6, Proposition 2.4]. Consequently, \( \text{ed}(\beta) \leq 1 \) and thus \( \text{ed}(\alpha) \leq 1 \). This completes the proof of Proposition 5 and thus of Theorem 1. \( \square \)

Remark 7. The condition on \( F \) in Theorem 1 can be weakened slightly: our argument goes through, with only minor changes, under the assumption that \( F \) is a \( p \)-field for some

---

\(^2\)In the case where \( \text{char}(k) \neq 2, 3 \) or 5, see also [4, Proposition 1.1(3)].
prime $p \neq 3$ (not necessarily algebraically closed). Recall that a field $k$ is called a $p$-field if $[l : k]$ is a power of $p$ for every finite field extension $l/k$; see [14, Definition 4.1.11].

Remark 8. Proposition 5 fails for separable field extensions of degree $n \geq 6$. In fact, if $E/F$ is a general extension of degree $n$, then for any constructible extension $F'/F$,

$$\operatorname{ed}(E'/F') \geq \operatorname{ed}(S_n; 3) = \left\lfloor \frac{n}{3} \right\rfloor.$$ 

Here $\operatorname{ed}(S_n; 3)$ denotes the essential dimension of $S_n$ at 3, $\left\lfloor \frac{n}{3} \right\rfloor$ denotes the integer part of $\frac{n}{3}$, and we are assuming that $\operatorname{char}(k) \neq 3$; see [13, Corollary 4.2].

Remark 9. Generalizing Hermite’s theorem to field extensions of degree $n \geq 6$ is an interesting and largely open problem. The only known positive result in this direction is the classical theorem of Joubert [10] for $n = 6$. There are also negative results for some $n$. For an overview, see [3].

REFERENCES

[1] M. Artin, Algebra, Prentice Hall, Inc., Englewood Cliffs, NJ, 1991. MR1129886
[2] J. Buhler and Z. Reichstein, On the essential dimension of a finite group, Compositio Math. 106 (1997), no. 2, 159–179. MR1457337
[3] M. Brassil and Z. Reichstein, The Hermite-Joubert problem over $p$-closed fields, in Algebraic groups: structure and actions, 31–51, Proc. Sympos. Pure Math., 94, Amer. Math. Soc., Providence, RI, 2017. MR3645067
[4] A. Beauville, Finite subgroups of $\operatorname{PGL}_2(K)$, in Vector bundles and complex geometry, 23–29, Contemp. Math., 522, Amer. Math. Soc., Providence, RI, 2010. MR2681719
[5] G. Berhuy and G. Favi, Essential dimension: a functorial point of view (after A. Merkurjev), Doc. Math. 8 (2003), 279–330. MR2029168
[6] G. Berhuy and G. Favi, Essential dimension of cubics, J. Algebra 278 (2004), no. 1, 199–216. MR2068074
[7] D. F. Coray, Algebraic points on cubic hypersurfaces, Acta Arith. 30 (1976), 267–296. MR0429731
[8] D. F. Coray, Cubic hypersurfaces and a result of Hermite, Duke Math. J. 54 (1987), 657–670. MR0899410
[9] C. Hermite, Sur l’invariant du dix-huitième ordre des formes du cinquième degré, J. Crelle 59 (1861), 304-305.
[10] P. Joubert, Sur l’équation du sixième degré, C.-R. Acad. Sc. Paris 64 (1867), 1025-1029.
[11] J. Kollár, Unirationality of cubic hypersurfaces, J. Inst. Math. Jussieu 1 (2002), no. 3, 467–476. MR1956057
[12] H. Kraft, A result of Hermite and equations of degree 5 and 6, J. Algebra 297 (2006), 234–253. MR2206857
[13] A. Meyer and Z. Reichstein, The essential dimension of the normalizer of a maximal torus in the projective linear group, Algebra Number Theory 3, no. 4 (2009), 467–487.
[14] A. Päster, Quadratic forms with applications to algebraic geometry and topology, London Mathematical Society Lecture Note Series, 217, Cambridge Univ. Press, Cambridge, 1995. MR1366652 (97c:11046)
[15] Z. Reichstein, Essential dimension, in Proceedings of the International Congress of Mathematicians. Volume II, 162–188, Hindustan Book Agency, New Delhi. MR2827790
[16] J.-P. Serre, Extensions icosahédriques, in Seminar on Number Theory, 1979–1980 (French), Exp. 19, 7 pp, Univ. Bordeaux I, Talence. MR0604216
[17] J.-P. Serre, Galois cohomology, translated from the French by Patrick Ion and revised by the author, Springer, Berlin, 1997. MR1466966

---

3Some authors use the terms “$p$-closed field” or ”$p$-special field” in place of ”$p$-field”.

[18] J.-P. Serre, Cohomological invariants, Witt invariants, and trace forms, notes by Skip Garibaldi, in *Cohomological invariants in Galois cohomology*, 1–100, Univ. Lecture Ser., 28, Amer. Math. Soc., Providence, RI. MR1999384

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF BRITISH COLUMBIA, VANCOUVER, CANADA

E-mail address: mbrassil@math.ubc.ca, reichst@math.ubc.ca