COMPOSITIO MATHEMATICA

Irreducibility of polynomials over global fields is diophantine

Philip Dittmann

Compositio Math. **154** (2018), 761–772.

doi:10.1112/S0010437X17007977

FOUNDATION
COMPOSITIO
MATHEMATICA

LONDON
MATHEMATICAL
SOCIETY
EST. 1865

https://doi.org/10.1112/S0010437X17007977 Published online by Cambridge University Press

Compositio Math. 154 (2018) 761–772
doi:10.1112/S0010437X17007977

Irreducibility of polynomials over global fields is diophantine

Philip Dittmann

Abstract

Given a global field K and a positive integer n, we present a diophantine criterion for a polynomial in one variable of degree n over K not to have a root in K. This strengthens a result by Colliot-Thélène and Van Geel [Compositio Math. **151** (2015), 1965–1980] stating that the set of non-nth powers in a number field K is diophantine. We also deduce a diophantine criterion for a polynomial over K of given degree in a given number of variables to be irreducible. Our approach is based on a generalisation of the quaternion method used by Poonen and Koenigsmann for first-order definitions of $\mathbb{Z}$ in $\mathbb{Q}$.

1. Statement of results

We generalise methods of Poonen [Poo09] and Koenigsmann [Koe16] to prove the following theorem.

Theorem. *Let K be a global field, i.e. a number field or a function field in one variable over a finite field, and $n > 0$ a positive integer. Then the set*

$$\{(a_0,\dots,a_{n-1}) \in K^n \colon X^n + a_{n-1}X^{n-1} + \dots + a_0 \in K[X] \text{ has no zero in } K\}$$

is diophantine.

As usual, a subset $A \subseteq K^n$ is called *diophantine* if there exist $m \geqslant 0$ and a polynomial $F \in K[X_1,\dots,X_n,Y_1,\dots,Y_m]$ such that

$$A = \{(x_1,\dots,x_n) \in K^n \colon \exists y_1,\dots,y_m \in K(F(x_1,\dots,x_n,y_1,\dots,y_m) = 0)\}.$$

Equivalently, diophantine subsets of K^n are exactly those that are definable by an existential first-order formula (with parameters) in the language of rings (equivalently, a positive existential first-order formula), and we will frequently adopt this viewpoint, in particular when seeking uniformity between different fields.

In the theorem, the construction of the polynomial F, or equivalently the defining first-order formula, is explicit in principle, although we have not taken care to optimise the number of variables (quantifiers) necessary.

Received 15 February 2016, accepted in final form 3 October 2017, published online 8 March 2018.
2010 Mathematics Subject Classification 11U05 (primary), 11R52 (secondary).
Keywords: central simple algebra, definability, diophantine set.

The research for this article was supported by the University of Oxford Clarendon Fund and Merton College Oxford.

As an immediate corollary to the theorem we obtain the following.

Corollary. *For every global field K and $n > 0$, the set of non-nth powers in K is diophantine.*

This was previously proven in [CVG15] in the case of a number field. We can also translate the theorem into the terminology of mathematical logic.

Corollary. *Let K be a global field and $K^{**} \supseteq K^*$ any two fields which are both elementary extensions of K. Then K^* is relatively algebraically closed in K^{**}.*

This answers [Koe16, Question 25]. A simple model-theoretic argument yields the following statement on irreducibility.

Corollary. *Let K be a global field. There exists a diophantine criterion for a polynomial over K in an arbitrary number of variables to be irreducible. More formally, fix $r, d \geqslant 0$. Then the set*

$$\left\{(a_{i_1,\dots,i_r})_{0\leqslant i_1,\dots,i_r\leqslant d} \in K^{(d+1)^r} : \sum_{0\leqslant i_1,\dots,i_r\leqslant d} a_{i_1,\dots,i_r} X_1^{i_1}\cdots X_r^{i_r} \in K[X_1,\dots,X_r] \text{ is irreducible}\right\}$$

is diophantine.

2. Preliminaries on central simple algebras

In this section, we extend the methods pioneered in [Poo09] from quaternion algebras over $\mathbb{Q}$ to general central simple algebras of prime degree over global fields. We assume the reader to be familiar with the theory of central simple algebras; see for instance [GS06] for an introduction.

Let F be a field and A a (finite-dimensional) central simple algebra over F. Define

$$S(A/F) = \{\operatorname{Trd}(x) \colon x \in A, \operatorname{Nrd}(x) = 1\},$$

where Trd and Nrd are the reduced trace and norm, respectively.

Proposition 2.1. *Let L be a global field and A a central simple algebra over L of prime degree l. Then*

$$S(A/L) = \bigcap_{v \text{ a place of } L} S(A\otimes L_v/L_v)\cap L.$$

This proposition is well known for char $L \neq 2$ and $l = 2$ (the proof in this case can rely on the Hasse principle for quadratic forms), and this case has been exploited for first-order definitions of $\mathbb{Z}$ in $\mathbb{Q}$ (and more generally for rings of integers in number fields, see [Par13], since adapted to global fields of odd characteristic, see [EM16]). For the proof in the general case we quote two lemmas from the theory of central simple algebras.

Lemma 2.2 [Jac09, Theorem 4.12]. *Let D be a central division algebra of degree n over a field F, and let F' be a field of degree n over F. Then F' splits D if and only if F' can be embedded into D over F (i.e. there is a subalgebra of D isomorphic to F' over F).*

Lemma 2.3 [GS06, Proposition 2.6.3]. *Let A/F be a central simple algebra of degree n and $x \in A$. If $F' \subseteq A$ is commutative subalgebra which contains x and is a degree n field extension of F, then $\operatorname{Nrd}(x) = \mathrm{N}_{F'/F}(x)$ and $\operatorname{Trd}(x) = \operatorname{Tr}_{F'/F}(x)$. In particular, if n is prime and A is a division algebra, then $\operatorname{Nrd}(x) = x^n$ and $\operatorname{Trd}(x) = nx$ if $x \in F$ and otherwise $\operatorname{Nrd}(x) = \mathrm{N}_{F(x)/F}(x)$ and $\operatorname{Trd}(x) = \operatorname{Tr}_{F(x)/F}(x)$.*

https://doi.org/10.1112/S0010437X17007977 Published online by Cambridge University Press

We write $F(x)$ for the smallest subalgebra of A containing F and x; under the assumption that A is a division algebra of prime degree n, $F(x)$ is necessarily a commutative division algebra, i.e. a field. Then the degree $[F(x)\colon F]$ is either 1 or n, since A is a (left) $F(x)$-vector space and $n^2 = \dim_F A = \dim_{F(x)} A \cdot [F(x)\colon F]$ (cf. the usual tower law for field extensions).

Lastly, we need the following easy consequence of Krasner's lemma.

Lemma 2.4. *Let l be a prime number, L a global field, $a \in L$, and $v_1, \ldots, v_r$ places of L. For each i, let $f_i \in L_{v_i}[X]$ be a monic irreducible polynomial of degree l with constant coefficient $(-1)^l$ and X^{l-1}-coefficient $-a$. Then there exists a monic irreducible polynomial $f \in L[X]$ of degree l with constant coefficient $(-1)^l$ and X^{l-1}-coefficient $-a$ such that $L_{v_i}[X]/(f) \cong L_{v_i}[X]/(f_i)$, i.e. the completion above v_i of the global field $L[X]/(f)$ is unique and given by $L_{v_i}[X]/(f_i)$.*

Proof. Each f_i must automatically be separable, otherwise we would have to have $l = \operatorname{char} L$, $f_i = X^l + (-1)^l$, but then f_i would be reducible.

If the coefficients of f are v_1-adically sufficiently close to those of f_1, then f is irreducible in $L_{v_1}[X]$ and therefore in $L[X]$, and additionally $L_{v_1}[X]/(f) \cong L_{v_1}[X]/(f_1)$: this is a standard consequence of Krasner's lemma, see e.g. [Jac09, Exercise 9.8.7]; see also [NSW08, Lemma 8.1.6 and proof of Proposition 8.1.5]. (For archimedean places v_i, the statement is easily checked separately.)

By weak approximation, we can choose the coefficients of f to v_i-adically approximate the coefficients of f_i arbitrarily well simultaneously for all i. □

Proof of Proposition 2.1. This is a local–global principle. Note that there is nothing to show if A is isomorphic to the algebra of $l \times l$-matrices over L since the set on both sides is just L in this case. So let us assume that A is non-split over L; hence, since A has prime degree over L, A is a division algebra by Wedderburn's theorem (see e.g. [GS06, Theorem 2.1.3]). The inclusion $\subseteq$ is clear. For the other inclusion, consider an element $a \in L$ of the right-hand side. We want to show that $a \in S(A/L)$, i.e. that there exists $x \in A$ with $\operatorname{Nrd}(x) = 1$ and $\operatorname{Trd}(x) = a$. Let $v_1, \ldots, v_r$ be the ramified places of A. (The local condition is trivial at all other places.) For each v_i there exists an element $x_i \in A \otimes L_{v_i}$ of reduced norm 1 and reduced trace a. We can disregard the case where x_i is in the centre L_{v_i}, as the norm condition then forces $x_i^l = 1$, and if $l \neq \operatorname{char} L$, then the trace condition forces $x_i = a/l \in L$, or if $l = \operatorname{char} L$, then $x_i = 1 \in L$; in either case we are done globally.

Assume therefore that $x_i \notin L_{v_i}$, so $L_{v_i}(x_i)/L_{v_i}$ is a field extension of degree l which splits $A \otimes L_{v_i}$ (by Lemma 2.2), with $\mathrm{N}_{L_{v_i}(x)/L_{v_i}}(x) = 1$ and $\mathrm{Tr}_{L_{v_i}(x)/L_{v_i}}(x) = a$ (by Lemma 2.3). Write $f_i \in L_{v_i}[X]$ for the minimal polynomial of x_i; it is a monic irreducible polynomial of degree l with constant coefficient $(-1)^l$ and X^{l-1}-coefficient $-a$ for reasons of norm and trace.

Let $f \in L[X]$ be a polynomial as in Lemma 2.4, so $L' = L[X]/(f)$ is a degree l field extension of L with completions $L_{v_i}[X]/(f_i) \cong L_{v_i}(x_i)$ above each v_i. The element $\overline{X} \in L'$ has minimal polynomial f, hence $\mathrm{N}_{L'/L}(\overline{X}) = 1$ and $\mathrm{Tr}_{L'/L}(\overline{X}) = a$. The field L' splits A by the Hasse–Brauer–Noether theorem since it splits A everywhere locally, so L' embeds into A by Lemma 2.2, and the image of $\overline{X}$ under this embedding has reduced norm 1 and reduced trace a by Lemma 2.3. □

The idea behind this proof is already present in [Eis05, Theorem 3.1].

Next we investigate the local conditions $S(A/L_v)$. For a finite field $\mathbb{F}$, define

$$U_l(\mathbb{F}) = \{\mathrm{Tr}_{\mathbb{F}^{(l)}/\mathbb{F}}(x)\colon x \in \mathbb{F}^{(l)} \backslash \mathbb{F}, \mathrm{N}_{\mathbb{F}^{(l)}/\mathbb{F}}(x) = 1\} \subseteq \mathbb{F},$$

where we write $\mathbb{F}^{(l)}$ for the extension field of $\mathbb{F}$ of degree l (unique up to isomorphism).

https://doi.org/10.1112/S0010437X17007977 Published online by Cambridge University Press

The following is essentially [Poo09, Lemma 2.1].

Lemma 2.5. *Let A/F be a central simple algebra of prime degree l over a local field.*

(i) *If A is split, then $S(A/F) = F$.*

(ii) *If A is a division algebra, then for all irreducible monic polynomials $X^l + a_{l-1}X^{l-1} + \cdots + a_0$ with constant coefficient $a_0 = (-1)^l$ we have $-a_{l-1} \in S(A/F)$.*

(iii) *If A is a division algebra and F is non-archimedean, then $\mathcal{O} \supseteq S(A/F) \supseteq \mathrm{res}^{-1}(U_l(\mathbb{F}))$, where $\mathcal{O}$ is the valuation ring, $\mathbb{F}$ is the residue field, and $\mathrm{res}\colon \mathcal{O} \to \mathbb{F}$ is the residue map.*

Proof. In the split case, reduced norm and trace coincide with the usual matrix determinant and trace, and all monic polynomials of degree l do occur as characteristic polynomials.

For the second point, every monic irreducible polynomial f generates a field extension $F[x]/(f)$, and every such field extension splits A by the theory of central simple algebras over local fields (see e.g. [NSW08, Corollary 7.1.4]). Hence, by Lemma 2.2, $F[x]/(f)$ embeds into A, and then $-a_{l-1} \in S(A/F)$ by Lemma 2.3, where a_{l-1} is the coefficient of X^{l-1} in f.

For the case of a division algebra over a non-archimedean local field, let $x \in A$ with $\mathrm{Nrd}(x) = 1$. Then by Lemma 2.3 $\mathrm{N}_{F(x)/F}(x)^l = 1$, so x is contained in the valuation ring of the local field $F(x)$, therefore integral over $\mathcal{O}$ and hence has integral trace. This proves $S(A/F) \subseteq \mathcal{O}$. For the other inclusion, if $\overline{a} \in U_l(\mathbb{F})$ then there exists a monic irreducible polynomial $\overline{f} = X^n + \overline{a_{l-1}}X^{l-1} + \cdots + \overline{a_0} \in \mathbb{F}[X]$ with $\overline{a_{l-1}} = -\overline{a}$ and $\overline{a_0} = (-1)^l$. Any lift of $\overline{f}$ to $F[X]$ is irreducible over F (because it generates an unramified extension of degree l), hence any lift $a \in \mathcal{O}$ of $\overline{a}$ is in $S(A/F)$ by the second point. □

We can now give a satisfactory statement on $S(A/F)$ in the non-split local case.

Proposition 2.6. *Let A/F be a central division algebra of prime degree l over a non-archimedean local field.*

(i) *If $l > 2$, then $S(A/F)$ is equal to the valuation ring $\mathcal{O}$ of F.*

(ii) *If $l = 2$, write $V(A/F)$ for the topological interior of $S(A/F)$. We then have $V(A/F) - V(A/F) = \mathcal{O}$, where $V(A/F) - V(A/F)$ is the set of differences of two elements of $V(A/F)$.*

For the proof of the first point, it suffices to prove the following lemma.

Lemma 2.7. *For $l > 2$ and an arbitrary finite field $\mathbb{F}$, we have $U_l(\mathbb{F}) = \mathbb{F}$.*

Proof. This result is equivalent to showing that for any given $a \in \mathbb{F}$, there exists a monic irreducible polynomial $f \in \mathbb{F}[X]$ of degree l with X^{l-1}-coefficient $-a$ and constant coefficient -1. Let us write q for the cardinality of $\mathbb{F}$. If $l > 5$, or $l = 5$ and $q > 9$, the result follows from Theorem 2.8 below. The remaining cases for $l = 5$ we check by hand.

It remains to consider the case $l = 3$. If a polynomial $f_b = X^3 - aX^2 + bX - 1$ is not irreducible, it must be divisible by $X - c$ for some $c \in \mathbb{F}^\times$. However, for each c there exists exactly one f_b divisible by $X - c$. By counting, there exists an f_b which is not divisible by any $X - c$ and therefore irreducible. □

Theorem 2.8. *Let $\mathbb{F}$ be a finite field of cardinality q and $n > 0$.*

(i) *If $n \geqslant 5$ and $q > \left((n+1)/2\right)^2$, there exists a monic irreducible polynomial of degree n over $\mathbb{F}$ with any given non-zero constant coefficient and given X^{n-1}-coefficient.*

(ii) *If $n \geqslant 6$, the same is true without assumption on q.*

https://doi.org/10.1112/S0010437X17007977 Published online by Cambridge University Press

Proof. These are [Coh05, Corollaries 2.2 and 2.3]. □

Proof of Proposition 2.6. For $l > 2$, the claim follows from the third part of Lemmas 2.5 and 2.7, so let us consider $l = 2$. Write $\mathbb{F}$ for the residue field of F and pick a uniformiser π.

For $a \in 2 + \pi + \pi^2\mathcal{O}$, the polynomial $f = X^2 - aX + 1$ is irreducible, since $f(X+1) = X^2 - (a-2)X + (2-a)$ is irreducible by Eisenstein's criterion. Hence, by the second point of Lemma 2.5, we have $2+\pi+\pi^2\mathcal{O} \subseteq S(A/F)$, so $V(A/F)$ contains the element $b = 2+\pi$; likewise $-b \in V(A/F)$ by passing from f to $f(-X)$. Furthermore, we also have $V(A/F) \supseteq \mathrm{res}^{-1}(U_2(\mathbb{F}))$ by Lemma 2.5 since the right-hand side is open.

If $\mathbb{F}$ has cardinality greater than 11, then $U_2(\mathbb{F}) - U_2(\mathbb{F}) = \mathbb{F}$ by [Poo09, Lemma 2.3]. We can check exhaustively that for the remaining finite fields we have $(U_2(\mathbb{F}) \cup \{2, -2\}) - U_2(\mathbb{F}) = \mathbb{F}$. Hence

$$V(A/F) - V(A/F) \supseteq (\mathrm{res}^{-1}(U_2(\mathbb{F})) \cup \{b, -b\}) - \mathrm{res}^{-1}(U_2(\mathbb{F})) = \mathcal{O}. \qquad \square$$

This proof is adapted from the proof of Proposition 2.3 in [Par13]. A modification is necessary because the set V_v constructed there fails to be contained in the interior of $S(A/F)$, interfering with the application of approximation theorems later on.

For a central simple algebra A of prime degree l over a global field L, we define $T(A/L) = S(A/L)$ if $l > 2$ and $T(A/L) = S(A/L) - S(A/L)$ (the set of pairwise differences of elements of S) if $l = 2$.

Proposition 2.9. *If A/L splits at all real places of L (which is always the case if $l \neq 2$ or L is a global function field), then*

$$T(A/L) = \bigcap_{\mathfrak{q} \in \Delta_{A/L}} \mathcal{O}_{\mathfrak{q}} \cap L,$$

where $\Delta_{A/L}$ is the finite set of places of L at which A/L does not split.

Proof. For $l > 2$, this is immediate from Propositions 2.1 and 2.6, so consider the case $l = 2$. The inclusion $\subseteq$ is clear from Proposition 2.1 and Lemma 2.5, so let $x \in \bigcap_{\mathfrak{q}\in\Delta_{A/L}} \mathcal{O}_{\mathfrak{q}} \cap L$. For each $\mathfrak{q} \in \Delta_{A/L}$ we have $x \in \mathcal{O}_{\mathfrak{q}} = V(A/L_{\mathfrak{q}}) - V(A/L_{\mathfrak{q}})$ according to Proposition 2.6, so pick $a_{\mathfrak{q}} \in V(A/L_{\mathfrak{q}})$ such that $x + a_{\mathfrak{q}} \in V(A/L_{\mathfrak{q}})$. Since $\Delta_{A/L}$ is finite and the $V(A/L_{\mathfrak{q}})$ are open, we can use weak approximation to find $a \in L$ such that $a, x + a \in V(A/L_{\mathfrak{q}}) \subseteq S(A/L_{\mathfrak{q}})$ for all $\mathfrak{q} \in \Delta(A/L)$, hence $a, x + a \in S(A/L)$ by Proposition 2.1 and therefore $x \in T(A/L)$. □

For later use, we also record the following fact.

Proposition 2.10. *Assume K is global field of characteristic $p > 0$ and L/K is a finite inseparable extension. Then any central simple algebra A/K of degree p is split by L.*

Proof. By replacing K with the maximal separable subextension of L/K, we may assume that L/K is a purely inseparable proper extension. Since $[K^{1/p} \colon K] = p$, we now necessarily have $L \supset K^{1/p}$. Hence, the result follows from Lemma 2.11 below. □

Lemma 2.11 [Jac96, Theorem 4.1.8]. *Let F be a field of characteristic $p > 0$ and A/F be a central simple algebra of degree p. Then A is split by the field $F^{1/p}$.*

https://doi.org/10.1112/S0010437X17007977 Published online by Cambridge University Press

2.1 First-order definability

For what is to follow we will need that $S(A/F)$ is existentially first-order definable (in the language of rings) in terms of structure constants of A, i.e. $S(A/F)$ needs to be diophantine uniformly over central simple algebras of some prime degree l and uniformly over base fields. (Recall that structure constants with respect to a basis $(X_i)_{1\leqslant i\leqslant l^2}$ of A/F are the constants $(a_{ijk})_{1\leqslant i,j,k\leqslant l^2}$ in F such that $X_i \cdot X_j = \sum_k a_{ijk}X_k$.) It suffices to prove the following lemma.

Lemma 2.12. *The functions* Trd *and* Nrd *are uniformly quantifier-freely definable, i.e. for fixed l there exists a quantifier-free first-order formula τ in $l^6 + l^2 + 1$ variables such that if F is a field, $(a_{ijk})_{1\leqslant i,j,k\leqslant l^2}$ are structure constants of a central simple algebra A/F, $(b_i)_{1\leqslant i\leqslant l^2}$ is the basis expansion of an element $x \in A$, and $c \in F$ is arbitrary, then $F \models \tau(\overline{a}, \overline{b}, c)$ if and only if $c = \mathrm{Trd}(x)$, and there is likewise such a formula for* Nrd *in place of* Trd.

Proof. If (a_{ijk}) are the structure constants of $M_{l\times l}$ in the standard basis (i.e. the basis given by matrices with a single entry equal to 1 and all other entries 0), then the elements (b_i) are precisely the entries of the matrix $x \in M_{l\times l}$, and hence reduced norm and trace, which agree with matrix determinant and trace, are given by polynomial functions of the b_i.

If F is algebraically closed, then any central simple algebra of degree l is isomorphic to $M_{l\times l}$, i.e. there exists a base change matrix that transforms the situation to the previous one. Hence we can find an existential formula τ that works over algebraically closed fields: it asserts the existence of a base change transforming the a_{ijk} into the structure constants with respect to the standard basis, and c being the right polynomial function of the (transformed) b_i. By quantifier elimination, we can replace τ by a quantifier-free formula which is equivalent over algebraically closed fields.

This formula τ in fact works for all fields. For this it suffices to note that $\mathrm{Trd}_{A/F}(x) = \mathrm{Trd}_{A\otimes\overline{F}/\overline{F}}(x\otimes 1)$ and likewise for the reduced norm, and $F \models \tau(\overline{a}, \overline{b}, c)$ if and only if $\overline{F} \models \tau(\overline{a}, \overline{b}, c)$ since τ is quantifier-free. □

Consequently, the set $T(A/L)$ is existentially first-order definable, uniformly over A of some fixed prime degree l and global fields L. We can even require the defining formula to be positive and existential, since an inequality $x \neq 0$ may always be replaced by the equivalent $\exists y(x \cdot y = 1)$.

Corollary 2.13. *For any finite place $\mathfrak{p}$ of a global field K, the ring $\mathcal{O}_{\mathfrak{p}} \cap K$ is diophantine in K.*

Proof. Take a prime number l, e.g. $l = 2$, and pick two central simple algebras $A, A'/K$ of degree l splitting at all real places of K and such that $\Delta_{A/K} \cap \Delta_{A'/K} = \{\mathfrak{p}\}$. This is always possible by the characterisation of the Brauer group of global fields by Hasse invariants, see [NSW08, Theorem 8.1.17]. Then $T(A/K)+T(A'/K) = \mathcal{O}_{\mathfrak{p}} \cap K$, and this is positively existentially definable in K with parameters. □

Of course, this result is far from new: see, for instance, [Shl94, Theorem 4.4]. The proof is essentially the same as [Poo09, Remark 2.6].

For later use, we also spell out a definability result for cyclic algebras. Recall that for a field F and a cyclic extension M/F of degree l with a generator σ of $\mathrm{Gal}(M/F)$ and an element $a \in F$ the cyclic algebra (M, σ, a) is the F-algebra generated by M and an element y subject to the relations $y^l = a$ and $xy = y\sigma(x)$ for all $x \in M$. It is central simple of degree l.

https://doi.org/10.1112/S0010437X17007977 Published online by Cambridge University Press

Lemma 2.14. *Let K be a global field and M/K a cyclic extension of prime degree l with a generator σ of $\mathrm{Gal}(M/K)$. Then there is a positive existential formula $\varphi_{M,\sigma}(a,x)$ in the language of rings, with parameters from K, such that in any finite extension L/K and for any $a \in K$ the formula $\varphi_{M,\sigma}(a,\cdot)$ defines the set $T((M,\sigma,a)\otimes_K L/L)$.*

Proof. Fixing an irreducible polynomial over K with splitting field M, we can write structure constants for (M,σ,a) as polynomial expressions in a with parameters from K. These are then also structure constants for $(M,\sigma,a)\otimes_K L/L$. Now we can use the positive existential definition of T. □

3. An interlude in class field theory

Fix a global field K and $n > 1$. Also fix a prime $l \mid n$ for this section.

The entirety of this section is rather technical; we set up the necessary machinery from class field theory, notably describing certain ideal groups $I_{\mathfrak{m}}$ and H as well as field extensions M_i/K, which is needed for our main proofs in the next section, in particular the central Proposition 4.5.

Let us fix some notation. Write Σ for the set of places of K. If K is a number field, write $\Sigma_\infty \subset \Sigma$ for the set of archimedean places. If K is a global function field, arbitrarily fix Σ_∞ to be any finite non-empty subset of Σ. In either case, we call Σ_∞ the set of places at infinity.

Let $\mathcal{O}_K$ be the ring of elements of K integral at each place in $\Sigma\backslash\Sigma_\infty$; this is a Dedekind domain, and the prime ideals of $\mathcal{O}_K$ are in bijection to places in $\Sigma\backslash\Sigma_\infty$. This ring is the usual ring of integers in the number field case. In the case of function fields, $\mathcal{O}_K$ depends on the choice of Σ_∞.

Write $I_{\mathcal{O}_K}$ for the group of fractional ideals of $\mathcal{O}_K$, $P_{\mathcal{O}_K}$ for the subgroup of principal fractional ideals, and $\mathrm{Cl}(\mathcal{O}_K) = I_{\mathcal{O}_K}/P_{\mathcal{O}_K}$. In the number field case, this is the usual ideal class group and well known to be finite. In the function field case, this is not the usual divisor class group, since we are ignoring the places at infinity, but rather the Σ_∞-class group in the sense of [Ros02, ch. 14], essentially the divisor class group modulo the classes of prime divisors at infinity. It is finite by [Ros02, Corollary 2 to Proposition 14.1].

We now fix some field extensions of K for later use. Choose k such that $l^k > |\mathrm{Cl}(\mathcal{O}_K)| \cdot n!$. Find an abelian extension M/K with Galois group $\mathrm{Gal}(M/K) \cong (\mathbb{Z}/l\mathbb{Z})^k$ and such that M/K is completely split at all infinite places.

Lemma 3.1. *For any choice of k we can find such M.*

Proof. This follows from existence theorems in class field theory, e.g. the general version of the Grunwald–Wang theorem [NSW08, Theorem 9.2.8]. (Note that we are never in what is called the 'special case' there, since we are looking for an abelian extension whose Galois group has prime exponent.)

It is not hard to give an explicit argument in the present situation, using (the totally real part of) cyclotomic extensions in the number field case, and the analogous Carlitz module construction (see [Ros02, ch. 12]) over a suitable subfield $\mathbb{F}_p(T) \subseteq K$ in the function field case. □

Remark 3.2. This choice of a distinguished abelian extension of K is already present in previous papers, in the special case $l = k = 2$; most notably in [Par13, § 3.3], a field extension $K(\sqrt{a},\sqrt{b})/K$ is chosen. Likewise, the modulus 8 which appears throughout [Koe16] can be retrospectively explained by an implicit choice of field extension $\mathbb{Q}(\sqrt{2},\sqrt{-1})/\mathbb{Q}$. The paper [EM16] independently from us transfers some of the ideas of [Par13] to the setting of global

https://doi.org/10.1112/S0010437X17007977 Published online by Cambridge University Press

function fields. Note however that in our situation the analogy between function fields and number fields is more direct: we do not have to impose the condition that M be linearly disjoint from the Hilbert class field of K as in (the proof of) [Par13, Lemma 3.19], a condition that [EM16] changes in the function field situation.

Let us write $I_{\mathfrak{m}} \leqslant I_{\mathcal{O}_K}$ for the set of fractional ideals of $\mathcal{O}_K$ in which none of the prime ideals ramified in M/K occur in numerator or denominator. Then we obtain the well-known *Artin map*

$$I_{\mathfrak{m}} \to \operatorname{Gal}(M/K)$$

as the unique homomorphism sending an unramified prime ideal to its Frobenius element. (In the function field case, note that since all infinite places are completely split in M/K, this map is induced by the Artin map on divisors.) Write $H < I_{\mathfrak{m}}$ for the kernel of this map.

By the Chebotarev density theorem, the set of prime ideals (excluding those at infinity and ramified ones) mapping to a given element of $\operatorname{Gal}(M/K)$, i.e. in a given coset in I_m/H, has density $1/|\operatorname{Gal}(M/K)| = 1/|I_{\mathfrak{m}}/H| = l^{-k}$. (Throughout, it does not matter whether we choose natural or Dirichlet density.)

By class field theory (see e.g. [Lan70, X, § 2] for number fields and [Ros02, Theorem 9.23] for function fields), there exists a modulus or cycle $\mathfrak{m} = \sum_{\mathfrak{p}} n_{\mathfrak{p}}\mathfrak{p}$, a formal sum of places of K ramified in M with $n_{\mathfrak{p}} \geqslant 0$, such that H contains the subgroup $P_{\mathfrak{m}} = \{(a) \colon a \in U_{\mathfrak{m}}\}$, where

$$U_{\mathfrak{m}} = \{a \in K^{\times} \colon v_{\mathfrak{p}}(a-1) \geqslant n_{\mathfrak{p}} \text{ for all ramified } \mathfrak{p}\}.$$

The quotient group $I_{\mathfrak{m}}/P_{\mathfrak{m}}$, a *generalised ideal class group*, is finite.

Now choose subextensions $M_1, \ldots, M_k$ with $\operatorname{Gal}(M_i/K) \cong \mathbb{Z}/l\mathbb{Z}$ such that M is the composite of the M_i. Furthermore, fix a generator σ_i of $\operatorname{Gal}(M_i/K)$ for each i.

The rest of this section consists of two lemmas needed in the proof of Proposition 4.5.

Lemma 3.3. *Let $a \in K^{\times}$ such that $(a) \in I_{\mathfrak{m}}$ and $(a) \notin H$. Then there exist a place $\mathfrak{p} \notin \Sigma_{\infty}$ and an M_i such that the algebra (M_i, σ_i, a) is not split at $\mathfrak{p}$, and $a \notin \mathcal{O}_{\mathfrak{p}}^{\times}$.*

Proof. The fractional ideal (a) of $\mathcal{O}_K$ factors as a product of prime ideals of K unramified in M and not in Σ_{∞}. The group $I_{\mathfrak{m}}/H \cong \operatorname{Gal}(M/K) \cong (\mathbb{Z}/l\mathbb{Z})^k$ has exponent l, hence there exists a prime ideal $\mathfrak{p} \notin H$ that occurs in (a) with multiplicity not divisible by l since $(a) \notin H$.

The prime $\mathfrak{p}$ is not completely split in M since $\mathfrak{p} \notin H$, so there exists some M_i in which $\mathfrak{p}$ is inert, i.e. the local extension $M_iK_{\mathfrak{p}}/K_{\mathfrak{p}}$ is unramified of degree l. Therefore the group of local norms $\mathrm{N}_{M_iK_{\mathfrak{p}}/K_{\mathfrak{p}}}((M_iK_{\mathfrak{p}})^{\times}) \subseteq K_{\mathfrak{p}}^{\times}$ consists of the elements of l-divisible valuation; thus a is not a local norm and therefore (M_i, σ_i, a) is not split at $\mathfrak{p}$. □

Lemma 3.4. *Let $P \subset \Sigma \backslash \Sigma_{\infty}$ be a set of places of density at least $1/n!$. Then there exists $a \in K^{\times}$ such that $(a) \in I_{\mathfrak{m}}$, $(a) \notin H$ and all places $\mathfrak{p} \in \Sigma \backslash \Sigma_{\infty}$ with $a \notin \mathcal{O}_{\mathfrak{p}}^{\times}$ are in P.*

Proof. We may remove the finitely many places ramified in M/K from P without affecting the hypotheses.

The set P has density at least $1/n! > |\operatorname{Cl}(\mathcal{O}_K)|/|I_{\mathfrak{m}}/H|$. Since the set of prime ideals in each coset in $I_{\mathfrak{m}}/H$ has density $1/|I_{\mathfrak{m}}/H|$ as noted above, P contains prime ideals from at least $|\operatorname{Cl}(\mathcal{O}_K)| + 1$ different cosets; thus we may pick $\mathfrak{p}, \mathfrak{p}' \in P$ in different classes in $I_{\mathfrak{m}}/H$ and in the same class in $\operatorname{Cl}(\mathcal{O}_K)$.

Now $\mathfrak{p}\mathfrak{p}'^{-1}$ is a principal fractional ideal of $\mathcal{O}_K$; pick a generator a. By construction, this generator satisfies all of the requirements. □

https://doi.org/10.1112/S0010437X17007977 Published online by Cambridge University Press

4. A diophantine criterion for proper extensions of global fields

In this section we find an existential sentence that distinguishes the fixed global field K from its finite extensions of degree n, see Theorem 4.8.

Definition 4.1. Let L/K be an extension of degree n and $l \mid n$ a prime number. A prime ideal $\mathfrak{p}$ of K is *l-good* (for L) if it is unramified in L and for all prime ideals $\mathfrak{q}$ of L above $\mathfrak{p}$ the inertia degree $[\mathcal{O}_L/\mathfrak{q} : \mathcal{O}_K/\mathfrak{p}]$ is divisible by l.

The prime number $l \mid n$ is *admissible* (for L) if either:

(i) L/K is separable and the set of l-good prime ideals of K has density at least $1/n!$; or

(ii) L/K is inseparable and $l = \operatorname{char} K$.

Lemma 4.2. *For every L/K of degree n there exists an admissible $l \mid n$.*

Proof. If L/K is inseparable, then by basic field theory $\operatorname{char} K \mid n$, so $l = \operatorname{char} K$ is admissible. Let us now assume that L/K is separable.

Let L'/K be the Galois hull of L/K, $G = \operatorname{Gal}(L'/K)$, $H = \operatorname{Gal}(L'/L) \lneq G$. Then $|G| \leqslant n!$. Let $g \in G$ of prime power order l^r with $l \mid n$ such that no conjugate of g is in H. Existence of such g is assured by Theorem 4.3 below: an element g has no conjugate in H if and only if g has no fixed point in the left-multiplication action of G on $\Omega = G/H$. If $\mathfrak{q}$ is a prime ideal of L' above an unramified ideal $\mathfrak{p}$ of K such that $\operatorname{Frob}(\mathfrak{q}/\mathfrak{p})$ is conjugate to g, then the inertia degree $f(\mathfrak{q}/\mathfrak{p})$ is equal to $\operatorname{ord}(g) = l^r$, so for $\mathfrak{q}' = \mathfrak{q} \cap L$ we have $f(\mathfrak{q}'/\mathfrak{p}) \neq 1$ since $\operatorname{Frob}(\mathfrak{q}/\mathfrak{p}) \notin H$, and $f(\mathfrak{q}'/\mathfrak{p}) \mid l^r$, hence $l \mid f(\mathfrak{q}'/\mathfrak{p})$. The set of such prime ideals $\mathfrak{p}$ has density at least $1/n!$ by the Chebotarev density theorem. □

Theorem 4.3 (Fein–Kantor–Schacher). *Let G be a finite group acting transitively on a set Ω with $|\Omega| > 1$. Then there exists an element $g \in G$ of prime power order l^r, with $l \mid |\Omega|$, acting without fixed points on Ω.*

Remark 4.4. The paper [FKS81], in which this theorem was first proved, used it for a similar purpose as we do: classifying relative Brauer groups $\operatorname{Br}(L/K)$ of global fields. There appears to be no known proof of this theorem that does not use the classification of finite simple groups.

Proposition 4.5. *For a global field L/K consider the following statement, which we call $(\dagger)^l_{L/K}$.*

> *There exists an element $a \in K^\times$ such that $(a) \in I_\mathfrak{m}$, $(a) \notin H$ and for all i both a and $1/a$ are in $T((M_i, \sigma_i, a) \otimes_K L/L)$.*

Then this statement is false for $L = K$, and it is true if L/K is an extension of degree n with l admissible.

Proof. Let us first consider the case $L = K$, and assume there were a as in the statement. By Lemma 3.3 there exist an M_i and a place $\mathfrak{p} \notin \Sigma_\infty$ such that the algebra (M_i, σ_i, a) is not split at $\mathfrak{p}$ and $a \notin \mathcal{O}_\mathfrak{p}^\times$. Hence $a \notin T((M_i, \sigma_i, a))^\times$ by Proposition 2.9 in contradiction to our assumption on a.

Now consider the case of a proper extension L/K of degree n with l admissible. If L/K is inseparable and $l = \operatorname{char} K$, then Proposition 2.10 implies that all algebras (M_i, σ_i, a) are split over L, so any choice of a will do as long as $(a) \in I_\mathfrak{m}$, $(a) \notin H$. Such a is afforded by Lemma 3.4.

https://doi.org/10.1112/S0010437X17007977 Published online by Cambridge University Press

If L/K is separable, let $P \subseteq \Sigma\backslash\Sigma_\infty$ be the set of l-good primes; it has density at least $1/n!$. Therefore Lemma 3.4 is applicable, so we obtain $a \in K^\times$ such that $(a) \in I_\mathfrak{m}$, $(a) \notin H$ and all places $\mathfrak{p} \in \Sigma\backslash\Sigma_\infty$ such that $a \notin \mathcal{O}_\mathfrak{p}^\times$ are in P. We claim that a is as desired, so we must show that

$$a, \frac{1}{a} \in T((M_i, \sigma_i, a) \otimes_K L/L)$$

for all i. The algebras $(M_i, \sigma_i, a) \otimes_K L$ split at all infinite places of L by construction of the M_i, so by Proposition 2.9 it suffices to show that they split at all primes $\mathfrak{q}$ of L above primes $\mathfrak{p} \in \Sigma\backslash\Sigma_\infty$ with $a \notin \mathcal{O}_\mathfrak{p}^\times$. But all those $\mathfrak{p}$ are l-good, so $l \mid [L_\mathfrak{q} \colon K_\mathfrak{p}]$ and hence $L_\mathfrak{q}$ does split all (M_i, σ_i, a) by the theory of central simple algebras over local fields. □

Remark 4.6. The element a in the statement $(\dagger)^l_{L/K}$ can be multiplied by an arbitrary element of $\mathcal{O}_K^\times$, i.e. the statement is really one about the principal ideal (a). To see this, observe that T is invariant under multiplication by $\mathcal{O}_K^\times$, and the local splitting behaviour of (M_i, σ_i, a) at a prime $\mathfrak{p}$ unramified in M/K only depends on the valuation $v_\mathfrak{p}(a)$, since the local norm group contains the local unit group for unramified extensions.

For each class of ideals in the set $(I_\mathfrak{m}/P_\mathfrak{m})\backslash(H/P_\mathfrak{m})$ that contains a principal (fractional) ideal, fix a representative principal ideal (a_j) and a generator $a_j \in K^\times$ thereof. This is a finite list since $I_\mathfrak{m}/P_\mathfrak{m}$ is finite. Thus every principal ideal in $I_\mathfrak{m}\backslash H$ has the form $(a_j b)$ for some $b \in U_\mathfrak{m}$ and one of the a_j. Therefore, by Remark 4.6, we may rephrase the statement $(\dagger)^l_{L/K}$ as follows.

For some a_j, there exists a $b \in U_\mathfrak{m}$ such that for all i we have

$$a_j b, \frac{1}{a_j b} \in T((M_i, \sigma_i, a_j b) \otimes_K L/L).$$

This statement is of a very specific form; in fact, we will show that is equivalent to a certain system of polynomial equations $G_r(x_1, \ldots, x_s, y_1, \ldots, y_t) = 0$ having a solution in $K^s \times L^t$. We again adopt the viewpoint of first-order logic in phrasing and proving this expressibility result.

Lemma 4.7. *Consider the first-order language of pairs of rings, i.e. with signature $(+, \cdot, 0, 1, U)$, where U is a unary predicate for a distinguished subring. There exists a positive existential sentence $\psi_{K,n,l}$ in this language, with parameters from K, such that the condition $(\dagger)^l_{L/K}$ from Proposition 4.5 is expressed precisely by $(L, K) \models \psi_{K,n,l}$.*

Proof. We use the equivalent form of $(\dagger)^l_{L/K}$ introduced above. This statement is straightforwardly written as

$$\psi_{K,n,l} = \bigvee_j \exists b \Big(b \in U_\mathfrak{m} \wedge \bigwedge_i a_j b, \frac{1}{a_j b} \in T((M_i, \sigma_i, a_j b)) \Big),$$

where $b \in U_\mathfrak{m}$ can be phrased as a positive existential statement since $U_\mathfrak{m}$ is a diophantine subset of K by Corollary 2.13, and $a_j b \in T((M_i, \sigma_i, a_j b))$ can likewise be expressed by Lemma 2.14. □

Theorem 4.8. *There exists a positive existential sentence $\psi_{K,n}$ in the language of pairs of rings, with parameters from K, such that $(K, K) \models \neg\psi_{K,n}$, but $(L, K) \models \psi_{K,n}$ for all extensions L/K of degree n.*

Proof. Let $\psi_{K,n} = \bigvee_{l \mid n} \psi_{K,n,l}$. Now the statement is an immediate consequence of Proposition 4.5, Lemmas 4.7 and 4.2. □

https://doi.org/10.1112/S0010437X17007977 Published online by Cambridge University Press

5. Proof of the main results

Lemma 5.1. *Let $f \in K[X]$ be monic of degree $n > 1$, so $K[X]/(f)$ is a ring into which K embeds canonically. Then f has no root in K if and only if either $(K[X]/(f), K) \models \psi_{K,n}$ or f factors as $f = g \cdot h$ with $g, h \in K[X]$ of degree $< n-1$ with both g and h not having a root in K.*

Proof. Assume that f has a root $x \in K$. Then $K[X]/(X - x) \cong K$ is a homomorphic image of $K[X]/(f)$ preserving K. Since $(K, K) \models \neg\psi_{K,n}$ by Theorem 4.8, we obtain $(K[X]/(f), K) \not\models \psi_{K,n}$, since truth of positive existential sentences is preserved under taking homomorphic images. Furthermore f cannot factor as a product of two polynomials in $K[X]$ without roots in K.

For the converse direction, assume that f has no root in K. Then either f can be written as a product of two polynomials in $K[X]$ without roots (and therefore each of degree > 1), or f is irreducible. In the latter case $K[X]/(f)$ is a field of degree n over K, so $(K[X]/(f), K) \models \psi_{K,n}$ by Theorem 4.8. □

Now we can prove our main theorem.

Theorem 5.2. *There exists an existential first-order formula $\varphi_{K,n}(a_0, \dots, a_{n-1})$ in the language of rings, with parameters in K, such that $K \models \varphi_{K,n}(a_0, \dots, a_{n-1})$ if and only if the polynomial $f = X^n + a_{n-1}X^{n-1} + \cdots + a_0$ has no root in K.*

Proof. We translate the equivalent statement from Lemma 5.1. Note that $(K[X]/(f), K)$, as a structure in the language of pairs of rings, is quantifier-freely definable in K, since elements of $K[X]/(f)$ correspond in a straightforward way to n-tuples of elements of K, and the definitions of addition, multiplication, and the distinguished subset K are immediate.

Hence we obtain $\varphi_{K,2}(a_0, a_1)$ by rewriting $\big(K[X]/(X^2 + a_1X + a_0), K\big) \models \psi_{K,2}$ as a statement about K and similarly $\varphi_{K,3}(a_0, a_1, a_2)$, since polynomials of degree at most 3 cannot factor as polynomials of smaller degrees without roots. For $\varphi_{K,4}$, we have to allow for the possibility of a reducible polynomial of degree 4 without roots, so we rewrite the statement

$$\begin{aligned} &((K[X]/(X^4 + a_3X^3 + X^2a_2 + Xa_1 + x_0), K) \models \psi_{K,4}) \vee \\ &\quad \exists b_0, b_1, c_0, c_1 \big(X^4 + a_3X^3 + a_2X^2 + a_1X + a_0 \\ &\qquad\qquad = (X^2 + b_1X + b_0)(X^2 + c_1X + c_0) \wedge \varphi_{K,2}(b_0, b_1) \wedge \varphi_{K,2}(c_0, c_1)\big) \end{aligned}$$

as a first-order statement about K to obtain $\varphi_{K,4}$; this is again correct by Lemma 5.1. Inductively, we can construct $\varphi_{K,n}$ in this manner for all n. □

Corollary 5.3. *Let $K^{**} \supseteq K^*$ be any two fields which are both elementary extensions of K. Then K^* is relatively algebraically closed in K^{**}.*

Proof. Theorem 5.2 is also true in K^* and K^{**}, with the same formulae $\varphi_{K,n}$, by first-order transfer. Let $f = X^n + a_{n-1}X^{n-1} + \cdots a_0 \in K^*[X]$ be a polynomial without a root in K^*. Then $K^* \models \varphi_{K,n}(\mathbf{a})$, therefore $K^{**} \models \varphi_{K,n}(\mathbf{a})$ (since $\varphi_{K,n}$ is an existential formula), whence f does not have a root in K^{**} either. □

Corollary 5.4. *There exists a diophantine criterion for a polynomial over K in an arbitrary number of variables to be irreducible.*

Proof. Irreducibility is expressible by a universal first-order formula, since f being irreducible means that for all pairs of polynomials of smaller total degree, f is not equal to their product. By the Łoś–Tarski preservation theorem of model theory [Hod97, Corollary 5.4.5], this property is

https://doi.org/10.1112/S0010437X17007977 Published online by Cambridge University Press

expressible by an existential first-order formula with parameters if and only if for every $K^{**} \supseteq K^*$ with $K^{**}, K^* \succeq K$ every irreducible polynomial over K^* remains irreducible over K^{**}.

We shall now show that this condition follows from relative algebraic closedness. Consider an irreducible polynomial $f \in K^*[\mathbf{X}]$, and assume without loss of generality (after affine change of coordinates and rescaling) that f has constant coefficient 1. Then f factors into irreducible factors $f_1, \ldots, f_n \in \overline{K^*}[\mathbf{X}]$, each with constant coefficient 1, and these factors remain irreducible in $\overline{K^{**}}[\mathbf{X}]$. If f factors non-trivially as $g \cdot h$ in $K^{**}[\mathbf{X}]$, we may assume after rescaling that both g and h have constant coefficient 1, so g, h can be factored into products of the f_i in $\overline{K^{**}}[\mathbf{X}]$ since this is a unique factorisation domain. But then the coefficients of g and h are both in $\overline{K^*}$ and in K^{**}, so they are in K^*, contradicting f being irreducible. □

Acknowledgement

I would like to thank my PhD supervisor, Jochen Koenigsmann, for helpful discussions on the subject of this paper and comments on the exposition.

References

Coh05 S. D. Cohen, *Explicit theorems on generator polynomials*, Finite Fields Appl. (2005), 337–357.

CVG15 J.-L. Colliot-Thélène and J. Van Geel, *Le complémentaire des puissances n-ièmes dans un corps de nombres est un ensemble diophantien*, Compositio Math. **151** (2015), 1965–1980.

Eis05 K. Eisenträger, *Integrality at a prime for global fields and the perfect closure of global fields of characteristic $p > 2$*, J. Number Theory **114** (2005), 170–181.

EM16 K. Eisenträger and T. Morrison, *Universally and existentially definable subsets of global fields*, Math Res. Lett. (2017), to appear. Preprint (2016), arXiv:1609.09787 [math.NT].

FKS81 B. Fein, W. M. Kantor and M. Schacher, *Relative Brauer groups II*, J. Reine Angew. Math. **328** (1981), 39–57.

GS06 P. Gille and T. Szamuely, *Central simple algebras and Galois cohomology* (Cambridge University Press, Cambridge, 2006).

Hod97 W. Hodges, *A shorter model theory* (Cambridge University Press, Cambridge, 1997).

Jac96 N. Jacobson, *Finite-dimensional division algebras over fields* (Springer, Berlin, 1996).

Jac09 N. Jacobson, *Basic algebra II*, second edn (Dover Publications, Mineola, NY, 2009).

Koe16 J. Koenigsmann, *Defining $\mathbb{Z}$ in $\mathbb{Q}$*, Ann. of Math. (2) **183** (2016), 73–93.

Lan70 S. Lang, *Algebraic number theory* (Addison-Wesley, Reading, MA; London, 1970).

NSW08 J. Neukirch, A. Schmidt and K. Wingberg, *Cohomology of number fields*, second edition (Springer, Berlin, Heidelberg, 2008).

Par13 J. Park, *A universal first order formula defining the ring of integers in a number field*, Math. Res. Lett. **20** (2013), 961–980.

Poo09 B. Poonen, *Characterizing integers among rational numbers with a universal-existential formula*, Amer. J. Math. **131** (2009), 675–682.

Ros02 M. Rosen, *Number theory in function fields* (Springer, New York, London, 2002).

Shl94 A. Shlapentokh, *Diophantine classes of holomorphy rings of global fields*, J. Algebra **169** (1994), 139–175.

Philip Dittmann dittmann@maths.ox.ac.uk
Mathematical Institute, University of Oxford, Woodstock Road,
Oxford OX2 6GG, UK

https://doi.org/10.1112/S0010437X17007977 Published online by Cambridge University Press