High powers in endomorphism rings over Dedekind domains

Alexandru Chirvasitu

Abstract

Let $\mathbb{A}$ be a Dedekind domain and T an endomorphism of a finitely-generated projective $\mathbb{A}$-module. If T is an s^{th} power in $\mathrm{End}_{\mathbb{A}}(M)$ for s ranging over an infinite set $\mathcal{S}$ of positive integers, then (a) T decomposes as a direct sum of the zero operator and an invertible operator on a summand of M and (b) that summand is semisimple or of finite order if $\mathcal{S}$ is appropriately large (what this means depends on the structure of the additive and multiplicative groups of $\mathbb{A}$). This generalizes a result of M. Cavachi's to the effect that the only non-singular integer matrix that is an s^{th} power in $M_n(\mathbb{Z})$ for all s is the identity.

Key words: Dedekind domain; local field; global field; abstract curve; projective; finitely-generated; semisimple; Fitting lemma; valuation; prime ideal; supernatural number

MSC 2020: 13F05; 11F85; 11R04; 11R27; 16U60; 11D88; 13A18; 12J20; 16W60

Introduction

The original impetus for the note was provided by the remark [5] that the only non-singular integer-valued matrix that is an n^{th} power of an integer matrix for every n is the identity. Very short proofs exist ([7, e.g. pp.934-935]), but the problem suggests numerous follow-up questions:

(a) Is it enough to assume the matrix is an n^{th} power for just infinitely many n? *(no: -1 is a power with arbitrary odd exponent)*;

(b) How about an n^{th} power for all but finitely many n? *(yes; most proofs generalize in this fashion)*;

(c) Assuming only infinitely many exponents, and taking a cue from (a) above, does it follow that the matrix is of finite order in the general linear group? *(yes; a consequence of Theorem 1.3)*;

(d) If so, how does the order relate to the exponents in question? *(coprime to those primes dividing the exponents with arbitrarily high powers: Theorem 1.3 reformulates this in terms of supernatural numbers)*;

(e) What can one say if the matrix is singular? *(almost as much: it is diagonalizable over $\mathbb{Z}$ to* $\mathrm{diag}(0\cdots 0,\ 1\cdots 1)$*; a consequence of Theorem 1.3 again, but see also [20] for idempotence).*

More generally (and vaguely), it is tempting to abstract some of the arithmetic driving the phenomena above away from the specifics of the situation. To that end, the discussion below substitutes a Dedekind domain $\mathbb{A}$ for the integers and an endomorphism T of a finitely-generated projective $\mathbb{A}$-module for the matrix. The main result (Theorem 1.3) disentangles several threads that appear entwined in the original problem:

22 Nov 2023 04:01:26 PST
230907-Chirvasitu Version 2 - Submitted to J. Comm. Alg.

Theorem A *Let $\mathbb{A}$ be a Dedekind domain and $T \in \mathrm{End}_{\mathbb{A}}(M)$ an endomorphism of a finitely-generated projective $\mathbb{A}$-module M.*

(1) If an endomorphism T is an s^{th} power in $\mathrm{End}_{\mathbb{A}}(M)$ for arbitrarily large $s \in \mathbb{Z}_{>0}$, then T is the direct sum of the zero operator and an invertible operator on a summand of M.

(2) Consider an infinite set $\mathcal{S}$ of positive integers such that

$$\begin{aligned} \mathrm{char}(\mathbb{A}) = 0 \quad &\Rightarrow \quad \text{the group } (\mathbb{A}, +) \text{ has no non-trivial elements divisible by every } s \in \mathcal{S}; \\ \mathrm{char}(\mathbb{A}) = p > 0 \quad &\Rightarrow \quad \{n \mid p^n \text{ divides some } s \in \mathcal{S}\} \text{ is unbounded.} \end{aligned} \tag{0-1}$$

If $T = T_s^s$, $T_s \in \mathrm{End}_{\mathbb{A}}(M)$ for every $s \in \mathcal{S}$, then the invertible summand of the preceding point is semisimple.

(3) Consequently, if the only elements of the multiplicative group $\mathbb{A}^\times$ that are s^{th} powers for all $s \in \mathcal{S}$ are roots of unity, said invertible summand is in fact of finite order.

Moreover, that order is coprime to every prime p satisfying the right-hand condition in (0-1).

This makes it clear, in particular, that

- the direct-sum decomposition of part (1) is a rather general phenomenon, reminiscent of *Fitting*-type results (e.g. [12, (19.16)]);
- the semisimplicity of item (2) stems from an "additive" constraint on the exponents;
- while finally, the finite-order result in (3) is a byproduct of a constraint on the multiplicative group $\mathbb{A}^\times$ of units (which group is particularly simple when $\mathbb{A} = \mathbb{Z}$).

All of this specializes well to rings of integers in algebraic number fields (Example 1.6 and Corollaries 1.9 and 1.10), or in positive-characteristic global fields (Corollary 1.11), as well as local fields of either positive (Example 1.8) or vanishing (Example 1.7) characteristic.

Acknowledgements

I am grateful for valuable input from M. Cavachi, R. Kanda, M. Reyes and V. Trivedi.

This work is partially supported through NSF grant DMS-2011128.

1 Highly divisible semisimple operators

We assume some background on *Dedekind domains* (noetherian integrally closed domains of Krull dimension ≤ 1 [18, §I.3, Definition following Proposition 4]), such as the reader can find in countless sources: [1, Chapter 9], [6, §16.3], [18, §I.3], [14, Chapter 3], etc. [3, §VII.2.2, Theorem 1] and [13, Theorem 6.20] provide extensive lists of alternative characterizations.

Remark 1.1 As defined here, the class of Dedekind domains includes that of fields; sources differ on this: [1, Chapter 9], [18, §I.3], [14, Chapter 3] and [16, §I.3, Definition 1.3] agree, since they phrase the requirement via universal quantification over non-zero prime ideals, of which fields have none. On the other hand, because [1, sentence following Theorem 9.3], [6, §16.3] and [9, §I.3, Definition following Theorem 6.2A] (for instance) require that the Krull dimension be *exactly* 1 (rather than only ≤ 1), the resulting Dedekind domains cannot be fields.

Nothing below hinges crucially on the matter; having to make a choice for definiteness, we count fields among Dedekind domains. ♦

22 Nov 2023 04:01:26 PST
230907-Chirvasitu Version 2 - Submitted to J. Comm. Alg.

Recall in particular [6, §16.3, Proposition 21 and Theorem 22] that for a Dedekind domain $\mathbb{A}$ an $\mathbb{A}$-module M is

$$\begin{aligned} &\text{finitely-generated } \textit{projective } [6, \S10.5, \text{Definition preceding Corollary 31}] \iff \\ &\text{it is finitely-generated torsion-free} \iff \\ &M \cong \bigoplus_{s=1}^{r} I_s \text{ for ideals } I_s \trianglelefteq \mathbb{A} \iff \\ &M \cong \mathbb{A}^{r-1} \oplus (I_1 \cdots I_r), \end{aligned} \tag{1-1}$$

where the last summand is the product of the r ideals. If the I_s of (1-1) are non-zero, r is the *rank* [6, §12.1, Definition preceding Theorem 4] of M.

It will be convenient to use the language of *supernatural numbers* ([8, §22.8], [19, §1.3], etc.): formal products $\prod_p p^{n_p}$ over primes p, with exponents $n_p \in \mathbb{Z}_{\geq 0} \sqcup \{\infty\}$. For these, one can make sense in the obvious fashion of products, least common multiples

$$\operatorname{lcm}\left\{\prod p^{n_{p,i}} \mid i \in I\right\} := \prod p^{\sup_i n_{p,i}}$$

and greatest common divisors

$$\gcd\left\{\prod p^{n_{p,i}} \mid i \in I\right\} := \prod p^{\inf_i n_{p,i}}$$

and other such arithmetic notions. The usual *p-adic valuation* ν_p [8, Example 2.2.1 (a)] attached to a prime number p extends to supernatural numbers in the obvious fashion:

$$\nu_p\left(\prod_p p^{n_p}\right) := n_p.$$

We also borrow a piece of notation/terminology from [17, §10.1]: for a set Π of primes, a (supernatural) Π-*number* is one whose prime divisors all belong to Π, whereas a (supernatural) Π'-*number* is one whose prime divisors all lie outside of Π.

Finally, we introduce some language in line with the standard terminology on *divisible groups (or modules)* [6, §10.5, discussion preceding Proposition 36 and Example (4) following it].

Definition 1.2 Let $x \in \mathcal{M}$ be an element in a multiplicatively-written monoid.

(1) x is *s-divisible (in $\mathcal{M}$)* for a positive integer s if there is $y \in \mathcal{M}$ with $y^s = x$.

(2) Similarly, for a set $\mathcal{S}$ of positive integers, x is *$\mathcal{S}$-divisible (in $\mathcal{M}$)* if it is s-divisible for every $s \in \mathcal{S}$.

(3) x is *an arbitrarily high power* or *arbitrarily highly divisible* if it $\mathcal{S}$-divisible for some infinite set $\mathcal{S}$ of positive integers. ♦

Theorem 1.3 *Let $\mathbb{A}$ be a Dedekind domain and M a finitely-generated projective $\mathbb{A}$-module.*

(1) If $T \in \operatorname{End}_{\mathbb{A}}(M)$ is an arbitrarily high power, then $M = \ker T \oplus \operatorname{im} T$ and $T|_{\operatorname{im} T}$ is invertible.

22 Nov 2023 04:01:26 PST
230907-Chirvasitu Version 2 - Submitted to J. Comm. Alg.

(2) Consider an infinite set $\mathcal{S}$ of positive integers such that

$$\text{char}(\mathbb{A}) = 0 \quad \Rightarrow \quad \textit{the group } (\mathbb{A}, +) \textit{ has no non-trivial } \mathcal{S}\textit{-divisible elements;} \tag{1-2}$$

$$\text{char}(\mathbb{A}) = p > 0 \quad \Rightarrow \quad p \in \Pi_{\mathcal{S}} := \{\textit{primes } p \mid \nu_p \operatorname{lcm}(s \mid s \in \mathcal{S}) = \infty\}. \tag{1-3}$$

If $T \in \text{End}_{\mathbb{A}}(M)$ is $\mathcal{S}$-divisible in $\text{End}_{\mathbb{A}}(M)$, then the restriction $T|_{\text{im}(T)}$ of (1) is semisimple.

(3) If in addition $(A^\times/\text{torsion}(A^\times), \cdot)$ also has no non-trivial $\mathcal{S}$-divisible elements then for an $\mathcal{S}$-divisible $T \in \text{End}_{\mathbb{A}}(M)$ the restriction $T|_{\text{im}(T)}$ is of finite $\Pi'_{\mathcal{S}}$-order.

(4) Conversely, if T is a direct sum of the zero operator and an operator of finite order d, then T is an n^{th} power in $\text{End}_{\mathbb{A}}(M)$ for every n coprime to d.

The statement of Theorem 1.3 (2) is phrased so as to have (1-2) plug directly into the proof, but that condition has an alternative, perhaps more transparent (because more directly numerical) description.

Definition 1.4 The set of *local characteristics* of a domain $\mathbb{A}$ is

$$\text{lchar}(\mathbb{A}) := \{\text{char}(\mathbb{A}/\mathfrak{p}) \mid \{0\} \neq \mathfrak{p} \trianglelefteq \mathbb{A} \text{ prime}\}. \qquad \blacklozenge$$

Proposition 1.5 *For a Dedekind domain $\mathbb{A}$ the conditions (1-2) and (1-3) are jointly equivalent to*

$$\sum_{p \in \text{lchar}(\mathbb{A})} \sup_{s \in S} \nu_p(s) = \infty. \tag{1-4}$$

Proof In positive characteristic p the set $\text{lchar}(\mathbb{A})$ is the singleton $\{p\}$, and (1-4) obviously rephrases (1-3). Assuming henceforth that $\text{char}(\mathbb{A}) = 0$, note that every prime $p \in \mathbb{Z}_{>0} \subset \mathbb{A}$ belongs to only finitely many prime ideals. For that reason, (1-4) can also be rendered as

$$\sum_{\text{primes } \mathfrak{p} \trianglelefteq \mathbb{A}} \sup_{s \in S} \nu_{\text{char}(\mathbb{A}/\mathfrak{p})}(s) = \infty. \tag{1-5}$$

Or, in words, (at least) one of the following two conditions obtains:

(a) there is some prime ideal $\mathfrak{p} \trianglelefteq \mathbb{A}$ with

$$\{\nu_p(s) \mid s \in \mathcal{S}\} \text{ unbounded}, \quad p := \text{char}(\mathbb{A}/\mathfrak{p});$$

(b) the set of prime ideals $\mathfrak{p} \trianglelefteq \mathbb{A}$ containing some $s \in \mathcal{S}$ is infinite.

(1-2) $\Longrightarrow$ (1-5): The joint negation of (a) and (b) means that there is a positive integer n such that $\frac{s}{\gcd(s,n)}$, $s \in \mathcal{S}$ belong to no prime ideals of $\mathbb{A}$, and hence are invertible. $n \in \mathbb{Z} \subseteq \mathbb{A}$, then, will be $\mathcal{S}$-divisible.

(1-5) $\Longrightarrow$ (1-2): If (b) holds we are done, for an $\mathcal{S}$-divisible element $x \in \mathbb{A}$ would then belong to infinitely many prime ideals, as no non-zero x can (since for $x \neq 0$ the principal ideal (x) decomposes uniquely as a product finitely many prime ideals [16, §I.3, Corollary 3.9]).

Assume (a) holds instead. An $\mathcal{S}$-divisible element is then p^n-divisible for every n, hence belongs to the trivial [1, Corollary 10.18] intersection $\bigcap_n \mathfrak{p}^n \trianglelefteq \mathbb{A}$. ■

22 Nov 2023 04:01:26 PST
230907-Chirvasitu Version 2 - Submitted to J. Comm. Alg.

The setup of Theorem 1.3 might appear somewhat contrived, but it covers (for appropriate $\mathcal{S}$) the Dedekind domains of most interest in number theory: the rings of integers in either *local* or *global fields*.

Example 1.6 A *number field* $\mathbb{K}$ is a finite extension of the rationals [14, first sentence of Chapter 2], which we may as well assume embedded in $\mathbb{C}$. These are also the *global fields* of characteristic zero of [4, §II.12]. The corresponding *number ring* [14, following Corollary 1 to Theorem 2] $\mathcal{O}_{\mathbb{K}} \subset \mathbb{K}$, consisting of the algebraic integers in $\mathbb{K}$, is a Dedekind domain [14, Theorem 14].

Any infinite $\mathcal{S}$ will do: (1-2) obviously holds in its alternative incarnation as (1-4), since $\operatorname{lchar}(\mathcal{O}_{\mathbb{K}})$ consists of *all* primes. As for the infinite-power property in the statement of Theorem 1.3 (3), it follows from the fact that $\mathcal{O}^{\times}$ is finitely generated as an abelian group (this is Dirichlet's celebrated *Unit Theorem*, usually stated much more precisely than we have any need to [14, Theorem 38]). ♦

Example 1.7 For a prime p, consider a finite extension $\mathbb{K}$ of the field $\mathbb{Q}_p$ of *p-adic numbers* [16, §II.1]. It is complete with respect to the unique extension $|\cdot|$ to $\mathbb{K}$ [16, §II.4, Theorem 4.8] of the *p-adic norm* $|\cdot|_p$ of [16, §II.2]. Such $\mathbb{K}$ are precisely the characteristic-0 *local fields* of [16, §II.5] (or [4, Chapter VI, Introduction]).

The corresponding *discrete valuation ring*

$$\mathcal{O}_{\mathbb{K}} := \{x \in \mathbb{K} \mid |x| \leq 1\}$$

is a principal ideal domain [18, §I.1, Proposition 1] (so in particular Dedekind). An infinite $\mathcal{S} \subseteq \mathbb{Z}_{>0}$ satisfies (1-2) if and only if $p \in \Pi_{\mathcal{S}}$ (i.e. we can find $s \in S$ divisible by arbitrarily high powers of p), in which case the hypothesis of Theorem 1.3 (3) also holds.

The first claim follows immediately from the fact that positive integers coprime to p are invertible in $\mathcal{O}_{\mathbb{K}}$. To verify the second, recall the direct-product decomposition ([15, §III.1, Proposition 1.1] or [10, §15.1, (2')])

$$\mathcal{O}_{\mathbb{K}}^{\times} \cong (\text{finite cyclic group}) \times U_{\mathbb{K}}^{(1)}, \tag{1-6}$$

where the groups

$$U_{\mathbb{K}}^{(i)} := 1 + \mathfrak{m}^i, \quad i \geq 1, \quad \mathfrak{m} \subset \mathcal{O}_{\mathbb{K}} \text{ is the unique maximal ideal}$$

are introduced in [15, §III.1] (also [18, §IV.2] or [10, §15.1]; in the latter, $\mathsf{H}_i = U_{\mathbb{K}}^{(i)}$ and $\mathsf{H} = \mathsf{H}_1$). Similarly,

$$U_{\mathbb{K}}^{(1)} \cong (\text{finite cyclic } p\text{-group}) \times \mathbb{Z}_p^{[\mathbb{K}:\mathbb{Q}_p]}$$

by [18, §XIV.4, Proposition 10] or [10, §15.5, One-unit theorem], where $\mathbb{Z}_p = \mathcal{O}_{\mathbb{Q}_p}$ is the ring of p-adic integers, regarded here as a group with its additive structure. All in all,

$$\mathcal{O}_{\mathbb{K}}^{\times} \cong F \times \mathbb{Z}_p^{[\mathbb{K}:\mathbb{Q}_p]}, \quad F \text{ finite abelian},$$

whence the conclusion. ♦

Example 1.8 The substance of the discussion in Example 1.7 goes through (that is, Theorem 1.3 (3) applies precisely when $p \in \Pi_{\mathcal{S}}$) for rings of integers in *positive*-characteristic local fields: per [4, Chapter VI, Introduction], the fields $\mathbb{K} = \Bbbk((t))$ of Laurent power series over finite fields $\Bbbk$ (whereupon $\mathcal{O}_{\mathbb{K}} = \Bbbk[[t]]$, the ring of formal power series).

(1-6) holds just as before, since the cited references are characteristic-blind on that count. As for $U_{\mathbb{K}}^{(1)}$, it is this time simply a free $\mathbb{Z}_p$-module [10, §15.4, One-unit theorem] (albeit one of infinite rank this time). ♦

22 Nov 2023 04:01:26 PST
230907-Chirvasitu Version 2 - Submitted to J. Comm. Alg.

An application of Theorem 1.3 to Example 1.6 yields

Corollary 1.9 *Let M be a finitely-generated projective module over a number ring $\mathcal{O}_{\mathbb{K}}$ and $\mathcal{S}$ an infinite set of positive integers.*

An $\mathcal{S}$-divisible one-to-one $T \in \mathrm{End}_{\mathcal{O}_{\mathbb{K}}}(M)$ is of finite order coprime to every $p \in \Pi_{\mathcal{S}}$. In particular, $T = 1$ provided for every prime p, there are elements of $\mathcal{S}$ divisible by arbitrarily high powers of p.

Proof Example 1.6 notes that parts (2) and (3) of Theorem 1.3 apply to any infinite $\mathcal{S}$, and the non-singularity condition disposes of $\ker T$. ■

Specializing Corollary 1.9 further to $M := \mathcal{O}_{\mathbb{K}}^m$ provides the following generalization of [5] (which in turn can be recovered by setting $\mathbb{K} = \mathbb{Q}$):

Corollary 1.10 *Let $\mathcal{O}_{\mathbb{K}}$ be a number ring and m a positive integer. The only non-singular matrix in $M_m(\mathcal{O}_{\mathbb{K}})$ that is an n^{th} power therein for all but finitely many n is the identity.* ■

We will also consider Dedekind domains $\mathbb{A}$ whose quotient fields are finite extensions of $\Bbbk(t)$ (the fields featuring in the definition of an *abstract smooth curve* [9, §I.6, following Corollary 6.6]), for positive-characteristic $\Bbbk$. When $\Bbbk$ is finite these are also the positive-characteristic global fields [4, §II.12], "globalizing" Example 1.8 akin to the passage from Example 1.7 to Example 1.6.

Corollary 1.11 *Let $\mathbb{A}$ be a Dedekind domain whose field of fractions $\mathbb{K}$ is a finite extension of $\Bbbk(t)$ for $p := \mathrm{char}(\Bbbk) > 0$, and M a finitely-generated projective $\mathbb{A}$-module.*

(1) If $T \in \mathrm{End}_{\mathbb{A}}(M)$ is $\mathcal{S}$-divisible for an infinite $\mathcal{S} \subseteq \mathbb{Z}_{>0}$ with $p \in \Pi_{\mathcal{S}}$ then T is diagonalizable over the algebraic closure $\overline{\Bbbk}$ of $\Bbbk$.

(2) In particular, $T = 0 \oplus T'$ with T' of p-coprime finite order if the only $\mathcal{S}$-divisible roots of unity in $\Bbbk^{\times}$ are roots of unity (e.g. if $\Bbbk$ is finite or, more generally, algebraic over its prime field).

Proof All of this follows from Theorem 1.3 (and its proof) upon noting that the arbitrarily highly divisible elements of $\mathbb{K}^{\times}$ must be algebraic over $\Bbbk \subset \Bbbk(t) \subsetneq \mathbb{K}$. ■

The direct-sum decomposition of Theorem 1.3 (1) is fairly easily dispatched. It relies in part on the following simple general remark, itself a variant of the *Fitting lemma* (variants of which appear as [6, §15.1, Exercise 5], [11, §3.3, preceding Theorem 3.7], etc.):

Lemma 1.12 *Let M be a noetherian module over a commutative ring $\mathbb{A}$ and $T \in \mathrm{End}_{\mathbb{A}}(M)$.*

If the endomorphism $\overline{T}$ induced by T on $M/\ker T^n$ is onto for some n, then $M = \ker T^m \oplus \mathrm{im}\ T^m$ and $T|_{\mathrm{im}\ T^m}$ is an automorphism for $m \gg 0$.

Proof The already-cited [6, §15.1, Exercise 5] shows that

- the non-decreasing chain of submodules $\ker T^m$ stabilizes;
- the sum
$$\ker T^m + \mathrm{im}\ T^m \leq M, \quad m \gg 0 \tag{1-7}$$
is direct;
- and $\overline{T}$ is in fact an *auto*morphism of $M/\ker T^m$, $m \gg 0$.

22 Nov 2023 04:01:26 PST
230907-Chirvasitu Version 2 - Submitted to J. Comm. Alg.

The conclusion follows immediately:

$$\ker T^m + \text{im } T^m/\ker T^m = \text{im } \overline{T}^m = \text{im } \overline{T} = \ker T^m + \text{im } T/\ker T^m = M/\ker T^m,$$

so (1-7) cannot be proper. ■

Lemma 1.13 *Let $\mathbb{A}$ be a Dedekind domain with quotient field $\mathbb{K}$, M, T and $\mathcal{S}$ as in Theorem 1.3, and assume (1-2) and (1-3). Denote also by $\mathbb{A} \subseteq \overline{\mathbb{A}} \subset \overline{\mathbb{K}}$ the integral closure of $\mathbb{A}$ in the algebraic closure $\overline{\mathbb{K}} \supseteq \mathbb{K}$.*

If $T \in \text{End}_{\mathbb{A}}(M)$ is unipotent and $\mathcal{S}$-divisible in $\text{End}_{\overline{\mathbb{A}}}(M \otimes_{\mathbb{A}} \overline{\mathbb{A}})$ then it is the identity.

Proof Set $E := \text{End}_{\mathbb{A}}(M)$ and denote by subscripts modules obtained by scalar extension: $M_{\mathbb{K}} := M \otimes_{\mathbb{A}} \mathbb{K}$,

$$E_{\overline{\mathbb{A}}} := E \otimes_{\mathbb{A}} \overline{\mathbb{A}} \cong \text{End}_{\overline{\mathbb{A}}}\left(M_{\overline{\mathbb{A}}}\right),$$

and so on.

Fix $T_s \in E_{\overline{\mathbb{A}}}$ with $T_s^s = T$, $s \in \mathcal{S}$. The eigenvalues of T_s are roots of unity (since those of T are 1: this is what *unipotence* [2, §I.4] means). It follows that the semisimple factor R_s in the *multiplicative Jordan decomposition* [2, §I.4, Corollary 1 to Proposition 4.2] $T_s = R_s U_s$ belongs to $E_{\overline{\mathbb{A}}} \subset E_{\mathbb{K}} = \text{End}_{\mathbb{K}}(M_{\mathbb{K}})$ along with its inverse, so that $U_s \in E_{\overline{\mathbb{A}}}$ as well. Working with U_s in place of T_s, we may now assume the latter unipotent.

We argue inductively on the minimal n with $(T-1)^n = 0$, with the inductive step consisting of substituting $M' := M/\ker(T-1)$ (also torsion-free) for M and replacing T and T_s with the operators induced thereon. It will thus be enough to assume that $(T-1)^2 = 0$ (the base case of the induction).

M' (because it is finitely-generated torsion-free) being projective, there is a (non-canonical) decomposition $M \cong \ker(T-1) \oplus M'$ that transports over to $M_{\overline{\mathbb{A}}}$ and gives block upper-triangular decompositions

$$T = \begin{pmatrix} 1 & S \\ 0 & 1 \end{pmatrix}, \quad T_s = \begin{pmatrix} 1 & S_s \\ 0 & U_s \end{pmatrix}, \quad U_s^s = 1.$$

Consider the two cases:

(a) In characteristic 0 the U_s are identities (being both unipotent and of finite order) so that

$$\begin{aligned} T_s^s = T &\implies sS_s = S \\ &\implies S \text{ is } \mathcal{S}\text{-divisible in } \text{Hom}_{\overline{\mathbb{A}}}\left(M'_{\overline{\mathbb{A}}},\ \ker(T-1)_{\overline{\mathbb{A}}}\right) \cong \text{Hom}_A(M', \ker(T-1))_{\overline{\mathbb{A}}}. \end{aligned}$$

Since the morphism space is projective finitely-generated over $\mathbb{A}$, the latter's assumed $\mathcal{S}$-non-divisibility implies that S vanishes and hence $T = 1$.

(b) In characteristic $p > 0$ we still have

$$U_s^{p^{\nu_p(s)}} = 1, \ \forall s \in \mathcal{S},$$

since those powers of U_s are both unipotent and roots of unity of orders $\frac{s}{p^{\nu_p(s)}}$ (coprime to p). Because the U_s all operate on the same finite-dimensional vector space $M_{\mathbb{K}}$, there is some m such that

$$U_s^{p^m} = 1, \quad \forall s \in \mathcal{S}.$$

Our assumption that $p \in \Pi_{\mathcal{S}}$ implies that $\nu_p(s) > m$ for at least one $s \in \mathcal{S}$; S then vanishes, being a multiple of the p-divisible $\frac{s}{p^m}$.

22 Nov 2023 04:01:26 PST
230907-Chirvasitu Version 2 - Submitted to J. Comm. Alg.

This concludes the proof. ■

Proof of Theorem 1.3 **(4)** is immediate: if $M \cong \ker T \oplus P$ with $T|_P$ of order d, then $T = (T^m)^n$ whenever $mn = 1 \mod d$; if n and d are coprime then such an m always exists, hence the conclusion.

(1): Note first that if $T \in \mathrm{End}_{\mathbb{A}}(M)$ is nilpotent and arbitrarily highly divisible, then it vanishes. Indeed, the operators T and

$$T_s \in \mathrm{End}_{\mathbb{A}}(M), \quad T_s^s = T, \quad \forall s \in \mathcal{S}$$

on the r-dimensional ($r := \mathrm{rank}(M)$) vector space $M_{\mathbb{K}} := M \otimes_A \mathbb{K}$ over the quotient field $\mathbb{K}$ of $\mathbb{A}$ are all nilpotent, so [6, §12.3, Exercise 32] $T_s^r = 0$, $\forall s$. But then $T = T_s^s$ vanishes as soon as $s \geq r$.

In general, the preceding argument shows that the restriction of T to the *generalized kernel*

$$\ker_{gen} T := \{v \in M \mid T^n v = 0 \text{ for some } n\}$$

vanishes, so that $\ker_{gen} T = \ker T$. But then $\ker T$ and $\mathrm{im}\ T$ already intersect trivially and the sum

$$\ker T + \mathrm{im}\ T \leq M$$

is direct. We will then be able to conclude via Lemma 1.12 (and its proof) as soon as we argue that the operator $\overline{T}$ induced by T on $\overline{M} := M/\ker T$ is onto (and hence invertible).

To see this, note that $\overline{M}$ is again projective finitely generated, so that one can speak of determinants of operators thereon. Now, the principal ideal $(\det T) \trianglelefteq \mathbb{A}$ is an arbitrarily high power in the multiplicative group of *fractional ideals* [16, §I.3, Definition 3.7]:

$$(\det T) = (\det T_s)^s \trianglelefteq \mathbb{A}, \quad s \in \mathcal{S}.$$

That group being free abelian on the set of prime ideals [16, §I.3, Corollary 3.9], it follows that $\det T$ is invertible in $\mathbb{A}$.

Restricting T and all of the T_s to the summand $\mathrm{im}\ T \leq M$, we can (and throughout the remainder of the proof will) assume T invertible.

(2): Assuming invertibility, we prove semisimplicity. Extend $\mathbb{K}$ to an overfield L by adjoining the eigenvalues α_i of T. Those eigenvalues are integral over $\mathbb{A}$, by the familiar argument (via [1, Proposition 5.1], say): $\mathrm{End}_{\mathbb{A}}(M)$ is finitely-generated as an $\mathbb{A}$-module, hence so is the $\mathbb{A}$-submodule generated as an $\mathbb{A}$-algebra by T. In other words $\alpha_i \in \mathbb{B}$, the integral closure of $\mathbb{A}$ in L, itself a Dedekind domain [16, §I.12, Proposition 12.8].

Observe next that the hypothesis of Theorem 1.3 (2) transports over from $\mathbb{A}$ to $\mathbb{B}$: for (1-3) this is clear, since the two rings have the same characteristic, while for (1-2) the claim follows from Proposition 1.5 and the fact that every prime $\mathfrak{p} \trianglelefteq \mathbb{A}$ is contained in (and the intersection of $\mathbb{A}$ with) finitely many $\mathfrak{P}_i \trianglelefteq \mathbb{B}$ ([16, §I.8, following Proposition 8.1] or [1, Chapter 5, Exercise 15]).

The upshot of all of this is that we may substitute $\mathbb{B}$ and L for $\mathbb{A}$ and $\mathbb{K}$ respectively, or, what is more alphabetically economical, simply assume that $\alpha_i \in \mathbb{A}$. But then the factors of the multiplicative Jordan decomposition $T = RU$ both belong to $\mathrm{End}_{\mathbb{A}}(M)$, those of the analogous factorizations $T_s = R_s U_s$ belong to

$$\mathrm{End}_{\overline{\mathbb{A}}}(M \otimes_{\mathbb{A}} \overline{\mathbb{A}}), \quad \overline{\mathbb{A}} := \text{integral closure of } \mathbb{A} \text{ in the algebraic closure } \overline{\mathbb{K}} \supseteq \mathbb{K},$$

22 Nov 2023 04:01:26 PST
230907-Chirvasitu Version 2 - Submitted to J. Comm. Alg.

and we can conclude by applying Lemma 1.13 to the $\mathcal{S}$-divisibility $U = U_s^s$, $s \in \mathcal{S}$ of the unipotent operator U (in place of T) that $U = 1$.

(3): Because we are assuming that the only $\mathcal{S}$-divisible elements of $\mathbb{A}^\times$ are roots of unity, so is $\det T$ and hence also the eigenvalues of T. But then T is also semisimple by part (2), hence the finite-order claim.

As to the constraint on the order of T: for every $p \in \Pi_{\mathcal{S}}$ there is some s for which lifting to the s^{th} power annihilates the entire *p-primary component* of torsion$(A^\times)$ (i.e. the group of elements whose order is a power of p [6, §4.5, Example (2) following Corollary 20]), and hence the order of every s^{th} power is coprime to p. The conclusion follows from

$$(\det T_s)^s = \det T, \ \forall s.$$

This finishes the proof. ■

It is perhaps worth noting that occasionally, the multiplicative constraint of Theorem 1.3 (3) *follows* from the hypothesis of part (2):

Proposition 1.14 *Let $\mathcal{S} \subseteq \mathbb{Z}_{>0}$ and $\mathbb{A}$ a Dedekind domain with at least one finite residue field of characteristic $p \in \Pi_{\mathcal{S}}$.*

The hypotheses of Theorem 1.3 (2) and (3) are then met.

Proof The positive-characteristic branch (1-3) is obvious, (1-2) holds also by Proposition 1.5, and the hypothesis of Theorem 1.3 (3) (the fact that the $\mathcal{S}$-divisible elements of $\mathbb{A}^\times$ are roots of unity) follows from the corresponding claim for integer rings of local fields (Examples 1.7 and 1.8) and the embedding [1, Remark (1) following Theorem 10.17]

$$\mathbb{A} \hookrightarrow \text{localization } \mathbb{A}_{\mathfrak{p}} \hookrightarrow \mathfrak{p}\text{-adic completion } \widehat{\mathbb{A}}_{\mathfrak{p}} := \varprojlim_n \mathbb{A}/\mathfrak{p}^n$$

for some prime ideal $\mathfrak{p} \trianglelefteq \mathbb{A}$ with finite characteristic-p residue field $\mathbb{A}/\mathfrak{p}$. ■

References

[1] Michael F. Atiyah and I. G. Macdonald. Introduction to commutative algebra. Reading, Mass.-Menlo Park, Calif.-London-Don Mills, Ont.: Addison-Wesley Publishing Company (1969)., 1969. 2, 4, 8, 9

[2] Armand Borel. *Linear algebraic groups.*, volume 126 of *Grad. Texts Math.* New York etc.: Springer-Verlag, 2nd enlarged ed. edition, 1991. 7

[3] Nicolas Bourbaki. Elements of mathematics. Commutative algebra. English translation. Actualites scientifiques et industrielles, Hermann. Adiwes International Series in Mathematics. Paris: Hermann; Reading, Mass.: Addison-Wesley Publishing Company. XXIV, 625 p. (1972)., 1972. 2

[4] J. W. S. Cassels and A. Fröhlich. Algebraic number theory. Proceedings of an instructional conference organized by the London Mathematical Society (a NATO Advanced Study Institute) with the support of the International Mathematical Union. London and New York: Academic Press 1967. xviii, 366 p. 100 s. (1967)., 1967. 5, 6

[5] Marius Cavachi. Problem 11401. *Am. Math. Mon.*, 115(10):949, 2008. 1, 6

[6] David S. Dummit and Richard M. Foote. *Abstract algebra*. Chichester: Wiley, 3rd ed. edition, 2004. 2, 3, 6, 8, 9

[7] Gerald A. Edger, Doug Hensley, and Douglas B. West. Problems and solutions. *The American Mathematical Monthly*, 117(10):pp. 929–936, 2010. 1

[8] Michael D. Fried and Moshe Jarden. *Field arithmetic. Revised by Moshe Jarden*, volume 11 of *Ergeb. Math. Grenzgeb., 3. Folge*. Berlin: Springer, 3rd revised ed. edition, 2008. 3

[9] Robin Hartshorne. *Algebraic geometry*, volume 52 of *Grad. Texts Math.* Springer, Cham, 1977. 2, 6

[10] Helmut Hasse. *Number theory. English translation edited and prepared for publication by Horst Günter Zimmer. Corrected and enlarged translation of "Hasse, Zahlentheorie", 3rd ed., Akademie-Verlag, Berlin 1969*, volume 229 of *Grundlehren Math. Wiss.* Springer, Cham, 1980. 5

[11] Nathan Jacobson. *Basic algebra II.* New York, NY: W. H. Freeman and Company, 2nd ed. edition, 1989. 6

[12] T. Y. Lam. *A first course in noncommutative rings.*, volume 131 of *Grad. Texts Math.* New York, NY: Springer, 2nd ed. edition, 2001. 2

[13] Max D. Larsen and Paul J. McCarthy. *Multiplicative theory of ideals*, volume 43 of *Pure Appl. Math., Academic Press*. Academic Press, New York, NY, 1971. 2

[14] Daniel A. Marcus. *Number fields*. Universitext. Cham: Springer, 2nd edition edition, 2018. 2, 5

[15] Jürgen Neukirch. *Class field theory*, volume 280 of *Grundlehren Math. Wiss.* Springer, Cham, 1986. 5

[16] Jürgen Neukirch. *Algebraic number theory. Transl. from the German by Norbert Schappacher*, volume 322 of *Grundlehren Math. Wiss.* Berlin: Springer, 1999. 2, 4, 5, 8

[17] Jean-Pierre Serre. *Linear representations of finite groups. Translated from the French by Leonard L. Scott*, volume 42 of *Grad. Texts Math.* Springer, Cham, 1977. 3

[18] Jean-Pierre Serre. *Local fields. Translated from the French by Marvin Jay Greenberg*, volume 67 of *Grad. Texts Math.* Springer, Cham, 1979. 2, 5

[19] Jean-Pierre Serre. *Galois cohomology. Transl. from the French by Patrick Ion*. Berlin: Springer, 1997. 3

[20] Qiaochu Yuan (https://math.stackexchange.com/users/232/qiaochu yuan). Which integer matrices are kth powers for all k? https://math.stackexchange.com/a/4534849/867117, 2022. accessed 2023-08-26. 1

Department of Mathematics, University at Buffalo
Buffalo, NY 14260-2900, USA
E-mail address: achirvas@buffalo.edu

22 Nov 2023 04:01:26 PST
230907-Chirvasitu Version 2 - Submitted to J. Comm. Alg.