## Algebra

# On the number of generators of an algebra 

CrossMark

## Sur le nombre de générateurs d'une algèbre

Uriya A. First, Zinovy Reichstein ${ }^{1}$<br>Department of Mathematics, University of British Columbia, Vancouver, Canada

## A R T I C L E I N F O

## Article history:

Received 21 October 2016
Accepted after revision 29 November 2016
Available online 7 December 2016
Presented by Jean-Pierre Serre


#### Abstract

A classical theorem of Forster asserts that a finite module $M$ of rank $\leq n$ over a Noetherian ring of Krull dimension $d$ can be generated by $n+d$ elements. We prove a generalization of this result, with "module" replaced by "algebra". Here we allow arbitrary finite algebras, not necessarily unital, commutative or associative. Forster's theorem can be recovered as a special case by viewing a module as an algebra where the product of any two elements is 0 . © 2016 Académie des sciences. Published by Elsevier Masson SAS. All rights reserved.


## R É S U M É

Un théorème classique de Forster affirme que tout module $M$ de type fini et de rang $\leq n$ sur un anneau noethérien de dimension de Krull $d$ peut être engendré par $n+d$ éléments. Nous prouvons une généralisation de ce résultat où le mot «module» est remplacé par «algèbre». Les algèbres considérées ici sont de type fini, mais non nécessairement unitaires, commutatives ou même associatives. Le théorème de Forster peut être déduit du cas particulier où un module est vu comme une algèbre dont le produit de deux éléments quelconques est 0 .
© 2016 Académie des sciences. Published by Elsevier Masson SAS. All rights reserved.

## 1. Introduction

Throughout this paper, $R$ will denote a commutative Noetherian ring with 1 . For $\mathfrak{p} \in \operatorname{Spec} R, R(\mathfrak{p})$ will denote the fraction field of $R / \mathfrak{p}$. The starting point of this paper is the following classical theorem of Forster.

Theorem 1.1 ([3]). Suppose $R$ is Noetherian of Krull dimension $d$ and let $M$ be a finite $R$-module. If the $R(\mathfrak{p})$-module

$$
M(\mathfrak{p}):=M \otimes_{R} R(\mathfrak{p})
$$

can be generated by $n$ elements for every $\mathfrak{p} \in \operatorname{Max} R$, then $M$ can be generated by $n+d$ elements.

[^0]Swan [13] showed that Theorem 1.1 remains valid when the Krull dimension of $R$ is replaced by the dimension of Max $R .^{2}$ Further generalizations and refinements of Forster's Theorem can be found in [13,2,14,6]. This note offers yet another generalization, replacing the finite $R$-module $M$ by a finite $R$-algebra $A$, i.e. by a finitely generated $R$-module $A$ with an $R$-bilinear multiplication map $A \times A \rightarrow A$. This bilinear map can be arbitrary; we do not require $A$ to be commutative or associative, or to have a unit element. For $\mathfrak{p} \in \operatorname{Spec} R$, write $A(\mathfrak{p}):=A \otimes_{R} R(\mathfrak{p})$.

Theorem 1.2. Assume $\operatorname{dim} \operatorname{Max} R=d$ and let $A$ be a finite $R$-algebra such that $A(\mathfrak{p})$ can be generated by $n$ elements as a non-unital $R(\mathfrak{p})$-algebra for every $\mathfrak{p} \in \operatorname{Max} R$. Then $A$ can be generated by $n+d$ elements as a non-unital $R$-algebra.

In the case where the multiplication map $A \times A \rightarrow A$ is identically zero, we recover Forster's Theorem 1.1. Other applications of Theorem 1.2 can be found in Section 4. Before proceeding with the proof, we remark that our argument also proves the following variants of Theorem 1.2.
(i) If $A$ is a unital algebra, Theorem 1.2 remains valid if we replace "generated as a non-unital algebra" with "generated as a unital algebra".
(ii) Both the original and the unital versions of Theorem 1.2 remain valid in the setting of [13], where $A$ is equipped with a left $\Lambda$-module structure, $\Lambda$ being an $R$-algebra, and generation means generation as an $R$-algebra carrying an additional $\Lambda$-module structure. Note that, unlike [13, Theorem 1], we do not require $\Lambda$ to be finitely generated as an $R$-module.
(iii) More generally, $A$ can be taken to be a finite $R$-multialgebra, i.e. a finite right $R$-module equipped with an indexed family of homogeneous maps $\left\{f_{i}: A^{n_{i}} \rightarrow A\right\}_{i \in I}$. Here we say that $f: A^{k} \rightarrow A$ is $\left(m_{1}, \ldots, m_{k}\right)$-homogeneous, if $f\left(a_{1} r_{1}, \ldots, a_{k} r_{k}\right)=f\left(a_{1}, \ldots, a_{k}\right) r_{1}^{m_{1}} \ldots r_{k}^{m_{k}}$ for all $a_{1}, \ldots, a_{k} \in A$ and $r_{1}, \ldots, r_{k} \in R$. Note that $k=0$ is allowed; in this case $f$ can be any map from $A^{0}=0$ to $A$. The family $\left\{f_{i}\right\}_{i \in I}$ is clearly amenable to base change, hence $A(\mathfrak{p})$ carries the structure of an $R(\mathfrak{p})$-multialgebra. A multisubalgebra of $A$ is an $R$-submodule closed under each $f_{i}$, and the multisubalgebra generated by $S \subset A$ is the smallest multisubalgebra containing $S$. Multialgebras can be used to encode many types of structures. For example, a (non-unital) $R$-algebra structure on $A$ is a ( 1,1 )-homogeneous map $A^{2} \rightarrow A$, a unit element can be specified by a map $A^{0} \rightarrow A$, an involution by a (1)-homogeneous map $A \rightarrow A$, a quadratic Jordan algebra structure by a (2,1)-homogeneous map $A^{2} \rightarrow A$, etc. Furthermore, if $\Lambda$ is an associative $R$-algebra, then a left $\Lambda$-module structure, as in (ii), can be represented by the family of (1)-homogeneous maps $\left\{f_{\lambda}: A \rightarrow A\right\}_{\lambda \in \Lambda}$, given by $f_{\lambda}(a)=\lambda a$.

## 2. Preliminary lemmas

Let $A$ be a finite $R$-algebra. For $\mathfrak{p} \in \operatorname{Spec} R$ and $a \in A$, denote the image of $a$ in $A(\mathfrak{p})$ by $a(\mathfrak{p})$.
Lemma 2.1. Let $a_{1}, \ldots, a_{n} \in A$. Then $a_{1}, \ldots, a_{n}$ generate $A$ as an $R$-algebra if and only if for all $\mathfrak{p} \in \operatorname{Max} R$, the elements $a_{1}(\mathfrak{p}), \ldots, a_{n}(\mathfrak{p})$ generate $A(\mathfrak{p})$ as an $R(\mathfrak{p})$-algebra.

Proof. Let $B$ be the $R$-subalgebra generated by $a_{1}, \ldots, a_{n}$. The map $B(\mathfrak{p}) \rightarrow A(\mathfrak{p})$ induced by the inclusion $B \hookrightarrow A$ is an isomorphism for all $\mathfrak{p}$. Since $A$ is a finite $R$-algebra, Nakayama's Lemma implies that the map $B_{\mathfrak{p}} \rightarrow A_{\mathfrak{p}}$ is an isomorphism for all $\mathfrak{p} \in \operatorname{Max} R$. It is well known that this implies $B=A$.

Lemma 2.2. Suppose $a_{1}, \ldots, a_{n} \in A$ and $\mathfrak{p} \in \operatorname{Spec} R$. If $a_{1}(\mathfrak{p}), \ldots, a_{n}(\mathfrak{p})$ generate $A(\mathfrak{p})$ as an $R(\mathfrak{p})$-algebra, then there exists an open neighborhood $U$ of $\mathfrak{p}$ in $\operatorname{Spec} R$ such that $a_{1}(\mathfrak{q}), \ldots, a_{n}(\mathfrak{q})$ generate $A(\mathfrak{q})$ for any $\mathfrak{q} \in U$.

Proof. By our assumption, there exist (non-associative) monomials $\omega_{1}, \ldots, \omega_{t}$ on $n$ letters such that $A(\mathfrak{p})$ is spanned by $\left\{\omega_{i}\left(a_{1}(\mathfrak{p}), \ldots, a_{n}(\mathfrak{p})\right)\right\}_{i=1}^{t}$ as an $R(\mathfrak{p})$-module. Write $b_{i}=\omega_{i}\left(a_{1}, \ldots, a_{n}\right)$. By Nakayama's Lemma, $A_{\mathfrak{p}}$ is spanned as an $R_{\mathfrak{p}}$-module by the images of $b_{1}, \ldots, b_{t}$. Let $B=\sum_{i} b_{i} R$. Then $(A / B)_{\mathfrak{p}}=0$. Since $A$ is finitely generated, there is $s \in R \backslash \mathfrak{p}$ such that $(A / B) s=0$. Thus, for any $\mathfrak{q} \in \operatorname{Spec} R$ not containing $s$, we have $(A / B)_{\mathfrak{q}}=0$. Hence, $a_{1}(\mathfrak{q}), \ldots, a_{n}(\mathfrak{q})$ generate $A(\mathfrak{q})$ as an $R(q)$-algebra.

To state the next lemma, we need some additional notations. Let $n \in \mathbb{N}$. For any commutative associative unital $R$-algebra $S$, let $A_{S}=A \otimes_{R} S$ and write

$$
V_{n}(S)=\left\{\left(a_{1}, \ldots, a_{n}\right) \in A_{S}^{n}: a_{1}, \ldots, a_{n} \text { generate } A_{S} \text { as an } S \text {-algebra }\right\} .
$$

For all $0 \leq i \leq n$, we further let

$$
V_{n, i}(S)=\left\{\left(a_{1}, \ldots, a_{i}\right) \in A_{S}^{i}: \exists a_{i+1}, \ldots, a_{n} \in A_{S} \text { such that }\left(a_{1}, \ldots, a_{n}\right) \in V_{n}(S)\right\}
$$

[^1]Lemma 2.3. Let $\mathfrak{p} \in \operatorname{Spec} R$, let $a_{1}, \ldots, a_{i} \in A$, and assume that $\left(a_{1}(\mathfrak{p}), \ldots, a_{i}(\mathfrak{p})\right) \in V_{n, i}(R(\mathfrak{p}))$. Then there exists an open neighborhood $U$ of $\mathfrak{p}$ in $\operatorname{Spec} R$ such that $\left(a_{1}(\mathfrak{q}), \ldots, a_{i}(\mathfrak{q})\right) \in V_{n, i}(R(\mathfrak{q}))$ for all $\mathfrak{q} \in U$.

Proof. There are $b_{i+1}, \ldots, b_{n} \in A(\mathfrak{p})$ such that $a_{1}(\mathfrak{p}), \ldots, a_{i}(\mathfrak{p}), b_{i+1}, \ldots, b_{n}$ generate $A(\mathfrak{p})$. After multiplying $b_{i+1}, \ldots, b_{n}$ by suitable invertible elements of $R(\mathfrak{p})$, we may assume that each $b_{j}$ is the image of some element $a_{j} \in A$. By Lemma 2.2, there is an open neighborhood $U$ of $\mathfrak{p}$ such that, for all $\mathfrak{q} \in U$, the elements $a_{1}(\mathfrak{q}), \ldots, a_{n}(\mathfrak{q})$ generate $A(\mathfrak{q})$. In particular, $\left(a_{1}(\mathfrak{q}), \ldots, a_{i}(\mathfrak{q})\right) \in V_{n, i}(R(\mathfrak{q}))$.

## 3. Proof of Theorem 1.2

We claim that, for every $0 \leq j \leq n+d$, there exist elements $a_{1}, \ldots, a_{j} \in A$ and a partition of $X:=\operatorname{Max} R$ into locally closed subsets $X=\mathcal{F}_{0}^{(j)} \sqcup \mathcal{F}_{1}^{(j)} \sqcup \cdots \sqcup \mathcal{F}_{n}^{(j)}$ with the following properties:
(1) for any $i \geqslant 1$ and any $\mathfrak{p} \in \mathcal{F}_{i}^{(j)}$, there are $t_{1}, \ldots, t_{i} \in\{1, \ldots, j\}$ such that

$$
\left(a_{t_{1}}(\mathfrak{p}), \ldots, a_{t_{i}}(\mathfrak{p})\right) \in V_{n, i}(R(\mathfrak{p}))
$$

(2) $\operatorname{dim} \mathcal{F}_{i}^{(j)} \leq \operatorname{dim} X+i-j$ for every $0 \leq i<n$.

For $j=n+d$, condition (2) implies that $\mathcal{F}_{i}^{(n+d)}=\emptyset$ for all $0 \leq i<n$, hence $X=\mathcal{F}_{n}^{(n+d)}$. Condition (1) then tells us that for every $\mathfrak{p} \in X$, there are $t_{1}, \ldots, t_{n} \in\{1, \ldots, n+d\}$ such that $\left(a_{t_{1}}(\mathfrak{p}), \ldots, a_{t_{n}}(\mathfrak{p})\right) \in V_{n, n}(R(\mathfrak{p}))=V_{n}(R(\mathfrak{p}))$. In particular, $a_{1}(\mathfrak{p}), \ldots, a_{n+d}(\mathfrak{p})$ generate $A(\mathfrak{p})$ as an $R(\mathfrak{p})$-algebra for every $\mathfrak{p} \in X$. Lemma 2.1 now implies that $a_{1}, \ldots, a_{n+d}$ generate $A$ as an $R$-algebra, proving the theorem.

To prove the claim, we will construct the elements $a_{1}, \ldots, a_{j} \in A$ and the partition $X=\mathcal{F}_{0}^{(j)} \sqcup \mathcal{F}_{1}^{(j)} \sqcup \cdots \sqcup \mathcal{F}_{n}^{(j)}$ by induction on $j$. For the base case $j=0$, set $\mathcal{F}_{0}^{(0)}:=X$ and $\mathcal{F}_{1}^{(0)}=\cdots=\mathcal{F}_{n}^{(0)}:=\emptyset$. Condition (2) clearly holds and condition (1) follows from the assumption that $A(\mathfrak{p})$ is generated by $n$ elements for every $\mathfrak{p} \in X$.

For the induction step, assume that elements $a_{1}, \ldots, a_{j} \in A$ and a partition $X=\mathcal{F}_{0}^{(j)} \sqcup \mathcal{F}_{1}^{(j)} \sqcup \cdots \sqcup \mathcal{F}_{n}^{(j)}$ satisfying conditions (1) and (2) have been constructed for some $0 \leqslant j<n+d$. We shall choose an element $a_{j+1} \in A$ as follows. For each $0 \leqslant i<n$, choose finitely many distinct points $\mathfrak{p}_{i, 1}, \ldots, \mathfrak{p}_{i, N_{i}} \in \mathcal{F}_{i}^{(j)}$ meeting all irreducible components of $\mathcal{F}_{i}^{(j)}$ (here we are using our standing assumption that $R$ is Noetherian). By condition (1), for each point $\mathfrak{p}_{i, s}$, there exist integers $t_{1}, \ldots, t_{i} \in\{1, \ldots, j\}$ (depending on $i$ and $s$ ) such that $\left(a_{t_{1}}\left(\mathfrak{p}_{i, s}\right), \ldots, a_{t_{i}}\left(\mathfrak{p}_{i, s}\right)\right) \in V_{n, i}\left(R\left(\mathfrak{p}_{i, s}\right)\right)$. Therefore, for each point $\mathfrak{p}_{i, s}$, there exists $b_{i, s} \in A\left(\mathfrak{p}_{i, s}\right)$ such that $\left(a_{t_{1}}\left(\mathfrak{p}_{i, s}\right), \ldots, a_{t_{i}}\left(\mathfrak{p}_{i, s}\right), b_{i, s}\right) \in V_{n, i+1}\left(R\left(\mathfrak{p}_{i, s}\right)\right)$. Since the sets $\mathcal{F}_{0}^{(j)}, \mathcal{F}_{1}^{(j)}, \ldots, \mathcal{F}_{n-1}^{(j)}$ are disjoint, the points $\mathfrak{p}_{i, s}$ are all distinct. By the Chinese Remainder Theorem, there exists $a_{j+1} \in A$ such that $a_{j+1}\left(\mathfrak{p}_{i, s}\right)=b_{i, s}$ for every $i=1, \ldots, n-1$, and every $s=1, \ldots, N_{i}$.

Now, by Lemma 2.3, for each $i$ and $s$ as above, there is an open subset $U_{i, s}$ of $X$ containing $\mathfrak{p}_{i, s}$ such that

$$
\begin{equation*}
\left(a_{t_{1}}(\mathfrak{p}), \ldots, a_{t_{i}}(\mathfrak{p}), a_{j+1}(\mathfrak{p})\right) \in V_{i+1, n}(R(\mathfrak{p})) \tag{3.1}
\end{equation*}
$$

for all $\mathfrak{p} \in U_{i, s}$. Let $U_{i}$ be the union of $U_{i, s}$, as $s$ ranges from 1 to $N_{i}$, and set $U_{n}=\emptyset$. Now set

$$
\mathcal{F}_{i}^{(j+1)}:= \begin{cases}\left(\mathcal{F}_{i-1}^{(j)} \cap U_{i-1}\right) \cup\left(\mathcal{F}_{i}^{(j)} \backslash U_{i}\right) & \text { if } i=1, \ldots, n, \text { and }  \tag{3.2}\\ \mathcal{F}_{0}^{(j)} \backslash U_{0} & \text { if } i=0 .\end{cases}
$$

It is easy to see that $\left\{\mathcal{F}_{0}^{(j+1)}, \ldots, \mathcal{F}_{n}^{(j+1)}\right\}$ is a partition of $X$. Let $0 \leq i<n$. By our construction, $U_{i}$ meets all irreducible components of $\mathcal{F}_{i}^{(j)}$, hence

$$
\begin{equation*}
\operatorname{dim}\left(\mathcal{F}_{i}^{(j)} \backslash U_{i}\right) \leqslant \operatorname{dim}\left(\mathcal{F}_{i}^{(j)}\right)-1 \tag{3.3}
\end{equation*}
$$

Conditions (1), (2) for the elements $a_{1}, \ldots, a_{j}, a_{j+1} \in A$ and the partition $X=\bigsqcup_{i} \mathcal{F}_{i}^{(j+1)}$ now readily follow from (3.1), (3.2), and (3.3). This completes the proof of Theorem 1.2.

## 4. Applications

Let $A$ and $B$ be $R$-algebras. We say that $A$ is a form of $B$ (or equivalently, $B$ is a form of $A$ ) if there is a faithfully flat commutative unital $R$-algebra $S$ such that $A \otimes_{R} S \cong B \otimes_{R} S$ as $S$-algebras. For example, an Azumaya $R$-algebra of degree $n$ is a form of the matrix algebra $M_{n}(R)$, a finite étale $R$-algebra of rank $n$ is a form of $R \times \cdots \times R$ ( $n$ times), a Cayley $R$-algebra is a form of the split octonion algebra $\mathbb{O}_{R}$ (see [7, Corollary 4.11] or [9, Theorem 3.9]), and when $2 \in R^{\times}$, an Albert $R$-algebra is a form of the split Albert algebra $H_{3}\left(\mathbb{O}_{R}\right)$, where $H_{3}$ denotes the space of $3 \times 3$ Hermitian matrices (see [9, Theorem 6.9]).

Proposition 4.1. Let $A$ and $B$ be finite-dimensional algebras over an infinite field $F$ and assume $A$ is a form of $B$. If $B$ can be generated by $n$ elements, then $A$ can also be generated by $n$ elements.

Proof. Let $r:=\operatorname{dim}_{F}(A)=\operatorname{dim}_{F}(B)$. Choose an $F$-basis for $A$ and use it to identify $A$ with the $F$-points of the affine space $\mathbb{A}_{F}^{r}$. It is easy to see that there exists an open subscheme $U$ of $\left(\mathbb{A}_{F}^{r}\right)^{n}$ such that, for every field extension $K / F$, the $K$-points of $U$ are the $n$-tuples $\left(x_{1}, \ldots, x_{n}\right) \in A_{K}^{n}$ that generate $A_{K}$ as a $K$-algebra. Our goal is to show that $U$ has an $F$-point. Since $U$ is an open subscheme of an affine space and $F$ is an infinite field, it suffices to check that $U \neq \emptyset$.

Choose an $F$-field $K$ such that $A_{K} \cong B_{K}$. Since $B$ is generated by $n$ elements as an $F$-algebra, the same $n$ elements will generate $B_{K}$ as a $K$-algebra. As $A_{K} \cong B_{K}$, this implies that $U$ has a $K$-point. Hence $U \neq \emptyset$, as claimed.

Corollary 4.2. Assume the dimension of $\operatorname{Max} R$ is $d$. Then
(a) every Azumaya $R$-algebra is generated by $d+2$ elements,
(b) every Cayley $R$-algebra is generated by $d+3$ elements,
(c) every Albert $R$-algebra is generated by $d+3$ elements, provided $2 \in R^{\times, 3}$ and
(d) every finite étale $R$-algebra of rank $n$ is generated by $d+1$ elements, provided $R / \mathfrak{p}$ is infinite for any $\mathfrak{p} \in \operatorname{Max} R$.

We remind the reader that in the statement of the corollary, "generated" means "generated as a non-unital algebra"; allowing the use of the unit element in the proof does not improve the bounds. Note that, in (d), the assumption that $R / \mathfrak{p}$ is infinite is automatic if $R$ contains an infinite field.

Proof. By Theorem 1.2, it is enough to prove the corollary when $R$ is a field $F$, in which case $d=0$. We let $A$ denote an $F$-algebra that is Azumaya (resp. Cayley, Albert, étale of rank $n$ ).
(a) First note that $\mathrm{M}_{n}(F)$ is generated by the two matrices, $E_{1,1}$ and $E_{1,2}+\cdots+E_{n-1, n}+E_{n, 1}$. Here $E_{i, j}$ denotes the $n \times n$ matrix having 1 in the $(i, j)$-position and 0 elsewhere. Proposition 4.1 now tells us that when $F$ is infinite, any form of $\mathrm{M}_{n}(F)$ is also generated by two elements. When $F$ is a finite field, the only form of $\mathrm{M}_{n}(F)$ is $\mathrm{M}_{n}(F)$ itself, by Wedderburn's theorem, so we are done.
(b) By [11, §III.4], a Cayley $F$-algebra $A$ is formed from a central simple $F$-algebra $Q$ of degree 2 via the Cayley-Dickson process. In particular, $A$ is generated by one element over $Q$. As we saw in the proof of part (a), $Q$ is generated by two elements over $F$. Hence, $A$ is generated by three elements over $F$.
(c) A split Albert $F$-algebra is generated by three elements; see [8, p. 112]. By Proposition 4.1, this is also the case for any Albert $F$-algebra when $F$ is infinite. Thus we may assume that $F$ is finite. In this case, Serre's Conjecture I (proved by Steinberg) implies that every Albert $F$-algebra is split. Indeed, isomorphism classes of Albert $F$-algebras are classified by the first Galois cohomology set $\mathrm{H}^{1}(F, G)$, where $G$ is the split simply-connected algebraic group of type $\mathrm{F}_{4}$ defined over $F$ [5, Proposition 37.11]. By Serre's Conjecture $\mathrm{I}, \mathrm{H}^{1}(F, G)=0$ whenever $F$ has cohomological dimension $\leqslant 1$; see [12, Theorem III.2.2.1]. On the other hand, finite fields are of cohomological dimension $\leqslant 1$; see [4, Theorem 6.2.6, Proposition 6.2.3]. This shows that $A$ is split, thus completing the proof of part (c).
(d) We need to show that any étale $F$-algebra $A$ of rank $n$ over an infinite field $F$ is generated by a single element. By Proposition 4.1, we may assume that $A=F \times \cdots \times F$ ( $n$ times). In this case, $A$ is generated by any element $\left(\alpha_{1}, \ldots, \alpha_{n}\right)$ with distinct entries.

Remark 4.3. In part (d), the assumption that $R / \mathfrak{p}$ is infinite for any $\mathfrak{p} \in \operatorname{Spec} R$ cannot be removed in general. Indeed, when $R$ is a field $F$ with $q$ elements and $A=F \times \cdots \times F$, one needs at least $\left\lceil\log _{q}(n+1)\right\rceil$ generators, since $x^{q}=x$ for any $x \in A$. In fact, it can be shown that any étale $F$-algebra of rank $n$ can be generated by $\left\lceil\log _{q}(n+1)\right\rceil$ elements (or $\left\lceil\log _{q} n\right\rceil$ if the use of the unity is allowed). Thus, if we drop the assumption that $R / \mathfrak{p}$ is infinite in Corollary $4.2(\mathrm{~d})$, we can still assert that $A$ is generated by $d+\left\lceil\log _{q}(n+1)\right\rceil$ elements, where $q=\min _{\mathfrak{p} \in \operatorname{Max} R}|R / \mathfrak{p}|$.

Remark 4.4. Recall that a unital associative algebra $A$ is called separable if $A$ is projective relative to the left $A \otimes_{R} A^{\text {op }}$-module structure given by $\left(a \otimes b^{\mathrm{Op}}\right) x=a x b(a, b, x \in A)$. Examples of separable algebras include Azumaya and finite étale algebras; see [1] for further details. In the case where $\operatorname{dim} \operatorname{Max}(R)=d$ and $R$ has no finite homomorphic images, Corollary 4.2(a) can be generalized as follows: every finite separable $R$-algebra can be generated by $d+2$ elements. Indeed, by Theorem 1.2, it suffices to show that every separable algebra $B$ over an infinite field $F$ is generated by two elements. Let $K$ be an algebraic closure of $F$. By [1, Corollary 2.4], $B \otimes_{F} K$ is a product of matrix algebras $\mathrm{M}_{d_{1}}(K) \times \cdots \times \mathrm{M}_{d_{r}}(K)$. By Proposition 4.1, we may assume $B$ itself is a product of matrix algebras $\mathrm{M}_{d_{1}}(F) \times \cdots \times \mathrm{M}_{d_{r}}(F)$. In this case, a proof can be found in [10, Proposition 2.10].

## Acknowledgement

We are grateful to Thomas Rüd and the anonymous referee for their help with the exposition.

[^2]
## References

[1] F. DeMeyer, E. Ingraham, Separable Algebras Over Commutative Rings, Lect. Notes Math., vol. 181, Springer-Verlag, 1971. MR0280479.
[2] D. Eisenbud, E.G. Evans Jr., Generating modules efficiently: theorems from algebraic K-theory, J. Algebra 27 (1973) 278-305. MR0327742.
[3] O. Forster, Über die Anzahl der Erzeugenden eines Ideals in einem Noetherschen Ring, Math. Z. 84 (1964) 80-87. MR0163932.
[4] P. Gille, T. Szamuely, Central Simple Algebras and Galois Cohomology, Camb. Stud. Adv. Math. 101 (2006). MR2266528.
[5] M.-A. Knus, A. Merkurjev, M. Rost, J.-P. Tignol, The Book of Involutions, Colloq. Publ. - Amer. Math. Soc., vol. 44, 1998, with a preface in French by J. Tits. MR1632779.
[6] S. Kumar Upadhyay, S.D. Kumar, R. Sridharan, On the number of generators of a projective module, Proc. Indian Acad. Sci. Math. Sci. 123 (4) (2013) 469-478. MR3146601
[7] O. Loos, H.P. Petersson, M.L. Racine, Inner derivations of alternative algebras over commutative rings, Algebra Number Theory 2 (8) (2008) 927-968. MR2457357.
[8] K. McCrimmon, A Taste of Jordan Algebras, Universitext, Springer, New York, 2004. MR2014924.
[9] H. Petersson, Albert algebras, http://www.fernuni-hagen.de/petersson/download/alb-alg-ottawa-2012.pdf.
[10] Z. Reichstein, On automorphisms of matrix invariants, Trans. Amer. Math. Soc. 340 (1) (1993) 353-371. MR1124173.
[11] R.D. Schafer, An Introduction to Nonassociative Algebras, Dover, New York, 1995, corrected reprint of the 1966 original. MR1375235.
[12] J.-P. Serre, Galois Cohomology, Springer-Verlag, Berlin, 2002, corrected reprint of the 1997 English edition. MR1867431.
[13] R.G. Swan, The number of generators of a module, Math. Z. 102 (1967) 318-322. MR0218347.
[14] R.B. Warfield Jr., The number of generators of a module over a fully bounded ring, J. Algebra 66 (2) (1980) 425-447. MR0593603.


[^0]:    E-mail addresses: uriya.first@gmail.com (U.A. First), reichst@math.ubc.ca (Z. Reichstein).
    1 The second author has been partially supported by NSERC Discovery Grant 250217-2012.
    http://dx.doi.org/10.1016/j.crma.2016.11.015
    1631-073X/© 2016 Académie des sciences. Published by Elsevier Masson SAS. All rights reserved.

[^1]:    ${ }^{2}$ Recall that the dimension of a topological space $X$ is the maximal length $d$ of a chain $\emptyset \neq X_{0} \subsetneq X_{1} \subsetneq \cdots \subsetneq X_{d} \subseteq X$ of closed irreducible subsets (or $-\infty)$. The Krull dimension of $R$ is the dimension of $\operatorname{Spec} R$ endowed with the Zariski topology. The maximal spectrum Max $R$ is a subspace of Spec $R$, hence $\operatorname{dim} \operatorname{Max} R \leqslant \operatorname{dim} \operatorname{Spec} R$.

[^2]:    ${ }^{3}$ If 2 is not invertible in $R$, then an Albert $R$-algebra should be regarded as quadratic Jordan algebra [9, Section 4]; cf. Remark (iii) in the Introduction.

