THE MODULI SPACE OF COMMUTATIVE ALGEBRAS OF FINITE RANK

BJORN POONEN

ABSTRACT. The moduli space of rank-n commutative algebras equipped with an ordered basis is an affine scheme $\mathfrak{B}_n$ of finite type over $\mathbb{Z}$, with geometrically connected fibers. It is smooth if and only if $n \le 3$. It is reducible if $n \ge 8$ (and the converse holds, at least if we remove the fibers above 2 and 3). The relative dimension of $\mathfrak{B}_n$ is $\frac{2}{27}n^3 + O(n^{8/3})$. The subscheme parameterizing étale algebras is isomorphic to GL_n/S_n, which is of dimension only n^2. For $n \ge 8$, there exist algebras that are not limits of étale algebras. The dimension calculations lead also to new asymptotic formulas for the number of commutative rings of order p^n and the dimension of the Hilbert scheme of n points in d-space for $d \ge n/2$.

This article has been published in *J. Europ. Math. Soc.* **10** (2008), no. 3, 817–836.

1. The moduli space of based algebras

All rings and algebras are assumed to be commutative, associative, and with 1, unless otherwise specified.

Let $n \in \mathbb{Z}_{\ge 0}$. For every ring k, we would like to parameterize the k-algebras that are locally free of rank n as a k-module. But for $n \ge 2$ this moduli problem turns out to be not representable by a scheme; the difficulty is related to presence of automorphisms. To rigidify, we equip k-algebras with extra structure. One option would be to consider k-algebras equipped with an ordered d-tuple of generators as a k-algebra: these are parameterized by the Hilbert scheme $\mathrm{Hilb}^n(\mathbb{A}^d)$ of n points in $\mathbb{A}^d$. Another option, the one explored in this paper, is to consider k-algebras equipped with an ordered basis.

Define a functor $\mathfrak{B}_n \colon \mathbf{Schemes}^{\mathrm{op}} \to \mathbf{Sets}$ as follows:

(1) If S is a scheme, an element of $\mathfrak{B}_n(S)$ is a pair $(\mathcal{A}, \phi)$ (strictly speaking, an isomorphism class of pairs) where $\mathcal{A}$ is an $\mathcal{O}_S$-algebra and $\phi \colon \mathcal{A} \to \mathcal{O}_S^{\oplus n}$ is an $\mathcal{O}_S$-module isomorphism. Two pairs $(\mathcal{A}, \phi)$ and $(\mathcal{A}', \phi')$ are considered the same if there is an isomorphism $\mathcal{A} \to \mathcal{A}'$ that with ϕ and ϕ' makes a commuting triangle.

(2) If $f \colon T \to S$ is a morphism of schemes, then $\mathfrak{B}_n(f) \colon \mathfrak{B}_n(S) \to \mathfrak{B}_n(T)$ maps $(\mathcal{A}, \phi)$ to $(f^*\mathcal{A}, f^*\phi)$.

Proposition 1.1. *The functor $\mathfrak{B}_n$ is representable by an affine scheme of finite type over $\mathbb{Z}$.*

Proof. Let $e_1, \ldots, e_n$ be the standard $\mathcal{O}_S$-basis of $\mathcal{O}_S^{\oplus n}$. Given $(\mathcal{A}, \phi) \in \mathfrak{B}_n(S)$, we may use ϕ to transport the multiplication on $\mathcal{A}$ to a multiplication on $\mathcal{O}_S^{\oplus n}$, which is described by giving the n^3 constants $c_{ij}^{\ell} \in H^0(S, \mathcal{O}_S)$ such that $e_i e_j = \sum_{\ell=1}^n c_{ij}^{\ell} e_\ell$; we also get $\phi(1) = \sum d_i e_i$ for some $d_i \in H^0(S, \mathcal{O}_S)$. Conversely, given elements $c_{ij}^{\ell}, d_i \in H^0(S, \mathcal{O}_S)$ satisfying the polynomial conditions that say that the resulting multiplication law is commutative and

Date: June 4, 2008; corrections July 29, 2021 and August 5, 2022.

2000 *Mathematics Subject Classification.* Primary 14D20; Secondary 13E10, 13M99, 14C05.

Key words and phrases. Hilbert scheme of points, finite-dimensional algebras, finite rings.

associative and has $\sum d_i e_i$ as a multiplicative identity, we can recover the algebra uniquely. Thus $\mathfrak{B}_n$ is representable by the closed subscheme of $\mathbb{A}_{\mathbb{Z}}^{n^3+n}$ cut out by these polynomial conditions on *indeterminates* c_{ij}^{ℓ} and d_i. □

From now on, $\mathfrak{B}_n$ denotes the representing scheme. Call $\mathfrak{B}_n$ the moduli space of based rank-n algebras.

Remark 1.2. Various analogues of $\mathfrak{B}_n$ have been studied in the literature before, at least over a base field. The paper [Fla68] defines the moduli space for based associative (but not necessarily commutative or unital) algebras, defines a GL_n-action as we do below, and studies GL_n-orbits in its irreducible components. The moduli space of based associative algebras with 1, along with the GL_n-action, is studied in [Gab74, Maz79, Maz82, LBR99]. In particular, [Maz79] contains a detailed study of its number of irreducible components and computes the number explicitly for $n = 5$ (it is 10). The paper [Maz80] studies the moduli space of based nilpotent commutative associative rank-n algebras over an algebraically closed field of characteristic not 2 or 3, especially for $n \leq 6$; it follows from this work that $\mathfrak{B}_n$ has geometrically irreducible fibers, at least over $\mathbb{Z}[1/6]$, for all $n \leq 7$. For an extensive survey of related work, see [Iar87]: there on page 311 it is written that "There is a virtually complete picture of isomorphism classes of Artin algebras and their deformations for $n \leq 8$, but that picture has never been written down in one place"; and presumably it is speaking of the case $k = \mathbb{C}$, but even in that case it seems that the published literature does not contain this. Asymptotic formulas for the dimension of $\mathfrak{B}_n$ and of the moduli space of based associative algebras with 1 are mentioned in [Ner87], whose primary goal was an asymptotic formula for the dimension of the moduli space of n-dimensional Lie algebras. Finally, the moduli space $\mathfrak{B}_n$ is implicit in some of the work of Bhargava [Bha04a, Bha04b, Bha04c, Bha05] on parameterizing and enumerating algebras of rank ≤ 5, especially over $\mathbb{Z}$.

Remark 1.3. Although we do not do it here, one should eventually try to define moduli spaces of algebras equipped with extra structure such as the resolvents in Bhargava's work, and also consider their quotients by a GL_n-action described below. Some of Bhargava's work may be interpreted as identifying such moduli spaces for $n \leq 5$ as quotients of affine space by a group acting linearly with a dense orbit. For $n > 5$, the classification of prehomogeneous vector spaces rules out such a simple interpretation, but it may still be possible to identify the moduli spaces as quotients of other simple varieties by group actions. This might yield an approach to counting rank-6 rings over $\mathbb{Z}$, for instance. That the situation for $n = 6$ should not be too bad is hinted at by [Poo08], which proves the finiteness of the set of isomorphism types of rank-6 algebras over any algebraically closed field.

On the other hand, the existence of "pathologies" such as reducibility of $\mathfrak{B}_n$ for higher n suggests that one should be careful in extrapolating the behavior of orders of number fields from the behavior for low degree. For one arithmetic application, see Proposition 9.7.

Definition 1.4. Given S, define two points of $\mathfrak{B}(S)$ as follows:

(1) $\tilde{\mathcal{A}}_{\mathrm{split}}$ is $\mathcal{A}_{\mathrm{split}} := \mathcal{O}_S \times \cdots \times \mathcal{O}_S$ equipped with the obvious basis.
(2) $\bullet$ is $\mathcal{A}_\bullet := \frac{\mathcal{O}_S[x_1,\dots,x_{n-1}]}{(x_1,\dots,x_{n-1})^2}$ equipped with the basis $1, x_1, \dots, x_{n-1}$.

For some calculations it will be simpler to work with based algebras where the first basis vector equals the multiplicative identity:

Definition 1.5. For $n \geq 1$, let $\mathfrak{B}_n^1$ be the scheme parameterizing based algebras such that the first basis vector equals 1. It is the closed subscheme of $\mathfrak{B}_n$ cut out by the equations $d_1 = 1$ and $d_i = 0$ for $i \geq 2$. For $n = 0$, we use the convention $\mathfrak{B}_0^1 := \mathfrak{B}_0$.

2. Action of the general linear group

Let GL_n be the general linear group scheme over $\mathbb{Z}$. Each $M \in \mathrm{GL}_n(S) = \mathrm{Aut}_{\mathcal{O}_S}(\mathcal{O}_S^{\oplus n})$ acts on $\mathfrak{B}_n(S)$ by sending $(\mathcal{A}, \phi)$ to $(\mathcal{A}, M \circ \phi)$. This defines a left action of GL_n on $\mathfrak{B}_n$.

Given two elements $(\mathcal{A}, \phi)$ and $(\mathcal{A}', \phi')$ of $\mathfrak{B}_n(S)$, the set $\mathrm{Isom}(\mathcal{A}, \mathcal{A}')$ of $\mathcal{O}_S$-algebra isomorphisms $\alpha\colon \mathcal{A} \to \mathcal{A}'$ is in bijection with the set of $M \in \mathrm{GL}_n(S)$ mapping $(\mathcal{A}, \phi)$ to $(\mathcal{A}', \phi')$. Namely, α corresponds to the $M \in \mathrm{GL}_n(S)$ making

$$\begin{array}{ccc} \mathcal{A} & \xrightarrow{\phi} & \mathcal{O}_S^{\oplus n} \\ {\scriptstyle\alpha}\downarrow & & \downarrow{\scriptstyle M} \\ \mathcal{A}' & \xrightarrow{\phi'} & \mathcal{O}_S^{\oplus n} \end{array}$$

commute.

It follows that the set of isomorphism classes of free rank-n $\mathcal{O}_S$-algebras is in bijection with the quotient set $\mathrm{GL}_n(S) \backslash \mathfrak{B}_n(S)$. Also, given $(\mathcal{A}, \phi) \in \mathfrak{B}_n(S)$, the group of $\mathcal{O}_S$-algebra automorphisms $\mathrm{Aut}(\mathcal{A})$ is identified with the stabilizer in $\mathrm{GL}_n(S)$ of $(\mathcal{A}, \phi) \in \mathfrak{B}_n(S)$.

3. Comparison of $\mathfrak{B}_n$ and $\mathfrak{B}_n^1$

For $n \geq 1$, let H be the subgroup scheme of GL_n stabilizing $(1, 0, \ldots, 0)$. It consists of invertible matrices whose first column equals $(1, 0, \ldots, 0)$. If $n = 0$, we use the convention that H, like GL_n, is the trivial group scheme. In any case, the relative dimension of H is $n^2 - n$.

The left action of GL_n on $\mathfrak{B}_n$ restricts to a left action of H on $\mathfrak{B}_n^1$. Also, there is a right action of H on GL_n given by multiplication on the right. Combining these gives a left H-action on $\mathrm{GL}_n \times \mathfrak{B}_n^1$ in which $N \in H(S)$ maps $(M, \tilde{\mathcal{A}}) \in (\mathrm{GL}_n \times \mathfrak{B}_n^1)(S)$ to $(MN^{-1}, N \cdot \tilde{\mathcal{A}})$. The contracted product $\mathrm{GL}_n \overset{H}{\wedge} \mathfrak{B}_n^1$ is the quotient of $\mathrm{GL}_n \times \mathfrak{B}_n^1$ by this (free) H-action.

Proposition 3.1. *The scheme* $\mathfrak{B}_n$ *is isomorphic to* $\mathrm{GL}_n \overset{H}{\wedge} \mathfrak{B}_n^1$.

Proof. Restricting the action $\mathrm{GL}_n \times \mathfrak{B}_n \to \mathfrak{B}_n$ yields a map

$$\mathrm{GL}_n \times \mathfrak{B}_n^1 \to \mathfrak{B}_n.$$

which is invariant for the H-action on $\mathrm{GL}_n \times \mathfrak{B}_n^1$. The fiber above $\tilde{\mathcal{A}} \in \mathfrak{B}_n(S)$ in $\mathrm{GL}_n \times \mathfrak{B}_n^1$ is a Zariski locally trivial torsor under H, trivialized by any open covering of S that splits the $\mathcal{O}_S$-module injection $\mathcal{O}_S \to \mathcal{A}$ given by the algebra structure. ☐

Definition 3.2. Define the moduli stack of locally free rank-n algebras as the Artin stack

$$\mathfrak{A}_n := [\mathrm{GL}_n \backslash \mathfrak{B}_n] \simeq [H \backslash \mathfrak{B}_n^1].$$

(Here \ denotes "stack quotient by the group acting on the left", not set difference!)

4. Comparison with Hilbert schemes

For any $n, d \in \mathbb{Z}_{\geq 0}$, let $\operatorname{Hilb}_n(\mathbb{A}^d)$ be the Hilbert scheme of n points in $\mathbb{A}^d$: it is the $\mathbb{Z}$-scheme whose S-points correspond (functorially in S) to closed subschemes T of $\mathbb{A}^d_S$ that are flat over S and whose geometric fibers have Hilbert polynomial equal to the constant polynomial n. Let $\mathfrak{H}_n(\mathbb{A}^d)$ be the $\mathbb{Z}$-scheme that parameterizes closed subschemes T as above equipped with an ordered $\mathcal{O}_S$-basis for $\mathcal{O}_T$. Then $\mathfrak{H}_n(\mathbb{A}^d)$ is a torsor under GL_n over $\operatorname{Hilb}_n(\mathbb{A}^d)$. There is a morphism $\mathfrak{H}_n(\mathbb{A}^d) \to \mathfrak{B}_n$ that maps $T \subseteq \mathbb{A}^d$ with an $\mathcal{O}_S$-basis to $\mathcal{O}_T$ with the $\mathcal{O}_S$-basis (forgetting the embedding into $\mathbb{A}^d$). This is GL_n-equivariant, so we obtain a cartesian diagram

$$\begin{array}{ccc} \mathfrak{H}_n(\mathbb{A}^d) & \longrightarrow & \mathfrak{B}_n \\ \downarrow & & \downarrow \\ \operatorname{Hilb}_n(\mathbb{A}^d) & \longrightarrow & \mathfrak{A}_n. \end{array}$$

We may view $\mathfrak{H}_n(\mathbb{A}^d)$ as the moduli space parameterizing rank-n $\mathcal{O}_S$-algebras $\mathcal{O}_T$ equipped with both a basis and a sequence $(x_1, \ldots, x_d)$ of global sections that generate $\mathcal{O}_T$ as an $\mathcal{O}_S$-algebra (to give these global sections is to give a closed immersion $T \hookrightarrow \mathbb{A}^d_S$). On the other hand, $\mathfrak{B}_n \times \mathbb{A}^{nd}$ is the moduli space parameterizing rank-n $\mathcal{O}_S$-algebras $\mathcal{O}_T$ equipped with both a basis and an *arbitrary* sequence $(x_1, \ldots, x_d)$ of global sections. (The nd coordinates on $\mathbb{A}^{nd}$ specify the coordinates of the x_i with respect to the basis.)

Proposition 4.1. *The morphism $\mathfrak{H}_n(\mathbb{A}^d) \to \mathfrak{B}_n \times \mathbb{A}^{nd}$ is an open immersion.*

Proof. Over a field k, the vector space spanned by the monomials of total degree $\leq e$ in $x_1, \ldots, x_d$ increases strictly in dimension with e until it stabilizes, so it must stabilize at or before $e = n - 1$. Thus $x_1, \ldots, x_d$ generate the rank-n k-algebra A if and only if the monomials of total degree $< n$ span A. This is a condition on the rank of a matrix whose entries are polynomials in the coordinates of the x_i with respect to a fixed basis of A; the condition is expressible as the nonvanishing of certain minors. Those minors, viewed as functions on $\mathfrak{B}_n \times \mathbb{A}^{nd}$, cut out the complement of $\mathfrak{H}_n(\mathbb{A}^d)$ in $\mathfrak{B}_n \times \mathbb{A}^{nd}$. □

Corollary 4.2. *The image of $\mathfrak{H}_n(\mathbb{A}^d) \to \mathfrak{B}_n$ is open in $\mathfrak{B}_n$.*

Proposition 4.3. *If $d \geq n$, then $\mathfrak{H}_n(\mathbb{A}^d) \to \mathfrak{B}_n$ admits a section. The map $\mathfrak{H}_n(\mathbb{A}^d) \to \mathfrak{B}_n$ is surjective if and only if $d \geq n - 1$.*

Proof. If $d \geq n$, define $\mathfrak{B}_n \to \mathfrak{H}_n(\mathbb{A}^d)$ by mapping an $\mathcal{O}_S$-algebra $\mathcal{A}$ with basis $e_1, \ldots, e_n$, to the same $\mathcal{O}_S$-algebra with the same basis and with algebra generators $(x_1, \ldots, x_d) := (e_1, \ldots, e_n, 0, 0, \ldots, 0)$; this is a section.

Given a based $\mathcal{O}_S$-algebra, Zariski locally on S we may replace one of the basis elements with 1 and still have a basis, and then the other basis elements are algebra generators. This proves surjectivity for $d \geq n - 1$.

We will not have surjectivity for $d < n - 1$, since $\mathcal{A}_\bullet$ cannot be generated as an algebra by fewer than $n - 1$ elements. □

Let k be a field. For any $\mathbb{Z}$-scheme V, let $V_k = V \underset{\operatorname{Spec} \mathbb{Z}}{\times} \operatorname{Spec} k$. For instance, $\mathfrak{B}_{n,k}$ denotes the k-variety (not necessarily irreducible) obtained from $\mathfrak{B}_n$.

Corollary 4.4. *We have*

$$\dim \mathrm{Hilb}_n(\mathbb{A}^d)_k \leq \dim \mathfrak{B}_{n,k} - n^2 + nd.$$

If $d \geq n-1$, then equality holds.

Proof. By Proposition 4.1,

$$\dim \mathrm{Hilb}_n(\mathbb{A}^d)_k = \dim \mathfrak{H}_n(\mathbb{A}^d)_k - \dim \mathrm{GL}_{n,k} \leq \dim \mathfrak{B}_{n,k} + \dim \mathbb{A}^{nd}_k - \dim \mathrm{GL}_{n,k}.$$

By 4.3, equality holds if $d \geq n-1$. □

Remark 4.5. If we are interested in only the case $n = d$, then the connection between Hilbert schemes and $\mathfrak{B}_n$ is even more direct. There is an open subscheme H_n of $\mathrm{Hilb}_n(\mathbb{A}^n)$ consisting of the points for which the corresponding quotient of the polynomial algebra is spanned as a vector space by the coordinate functions on $\mathbb{A}^n$. Also, for any rank-n algebra with a fixed basis, the locus of bases is contained in the locus of n-tuples of algebra generators, which is contained in the affine space of all n-tuples of elements, and the first is dense in the third, so the first is dense in the second, which implies that the open subscheme H_n of $\mathrm{Hilb}_n(\mathbb{A}^n)$ is Zariski dense. Now we have an isomorphism $\mathfrak{B}_n \simeq H_n$ taking a based algebra to the same algebra equipped with the n algebra generators given by the basis. This isomorphism may also be viewed as the composition of the section $\mathfrak{B}_n \to \mathfrak{H}_n(\mathbb{A}^n)$ of Proposition 4.3 with the morphism $\mathfrak{H}_n(\mathbb{A}^n) \to \mathrm{Hilb}_n(\mathbb{A}^n)$. The fact that $\mathfrak{B}_n$ is isomorphic to a dense open subscheme of $\mathrm{Hilb}_n(\mathbb{A}^n)$ explains why many of the properties of $\mathfrak{B}_n$ we prove in later sections reflect the corresponding properties of Hilbert schemes.

Remark 4.6. By [Fog68] (see especially Corollary 2.10 and the proof of Theorem 2.4 there), $\mathrm{Hilb}_n(\mathbb{A}^2)$ is smooth over $\mathbb{Z}$ with geometrically irreducible fibers. It follows that the same is true of $\mathfrak{H}_n(\mathbb{A}^2)$, and (by Proposition 4.1) of the image of $\mathfrak{H}_n(\mathbb{A}^2) \to \mathfrak{B}_n$ viewed as an open subscheme of $\mathfrak{B}_n$ (the locus parameterizing based algebras that can be locally generated as an algebra by ≤ 2 elements). If $n \leq 3$, Proposition 4.3 implies that this locus is the whole scheme $\mathfrak{B}_n$, which is then smooth over $\mathbb{Z}$ with geometrically irreducible fibers.

Remark 4.7. Fix a characteristic $p \geq 0$ and a nonnegative integer d. The value of $\dim \mathrm{Hilb}_n(X)$ is the same for every nonempty smooth variety X of dimension d over a field of characteristic p.

5. The moduli spaces for $n \leq 3$

Proposition 5.1. *For $n \leq 3$, the isomorphism type of the $\mathbb{Z}$-scheme $\mathfrak{B}^1_n$ is given by the following table:*

n	0	1	2	3
$\mathfrak{B}^1_n$	$\mathbb{A}^0$	$\mathbb{A}^0$	$\mathbb{A}^2$	$\mathbb{A}^6$

Proof. On $\mathfrak{B}^1_n \subseteq \mathfrak{B}_n \subseteq \mathbb{A}^{n^3+n}$ the values of the coordinates d_i are specified, and the values of c^ℓ_{ij} when i or j is 1 are forced by the defining polynomials. Thus we may view $\mathfrak{B}^1_n$ as a closed subscheme in the affine space $\mathbb{A}^{(n-1)^2 n}$ whose coordinates are the indeterminates c^ℓ_{ij} for $2 \leq i,j \leq n$ and $1 \leq \ell \leq n$.

When $n \leq 2$, the commutativity and associativity conditions on these c^ℓ_{ij} are vacuous, so $\mathfrak{B}^1_n \simeq \mathbb{A}^{(n-1)^2 n}$.

Finally, suppose $n = 3$. Call a basis for a rank-3 algebra good if it has the form $1, \alpha, \beta$ with $\alpha\beta \in \mathcal{O}_S \cdot 1$. We paraphrase [DF40, §15] (see also [GGS02, §4]), where it was shown that rank-3 algebras (over $\mathbb{Z}$) equipped with a good basis are in bijection with binary cubic forms. Let $\mathfrak{B}_3^{1,\mathrm{good}}$ be the closed subscheme of $\mathfrak{B}_3^1$ parameterizing rank-3 algebras equipped with a good basis. There is a left action of $\mathbb{G}_a^2$ on $\mathfrak{B}_3^1$ in which $(a,b) \in \mathbb{G}_a^2(S)$ maps an algebra $\mathcal{A}$ equipped with basis $1, \alpha, \beta$ to $\mathcal{A}$ equipped with basis $1, \alpha + a, \beta + b$. This action restricts to an isomorphism

$$\mathbb{G}_a^2 \times \mathfrak{B}_3^{1,\mathrm{good}} \to \mathfrak{B}_3^1.$$

Using the conditions coming from commutativity and associativity, one finds that the multiplication in any based algebra in $\mathfrak{B}_3^{1,\mathrm{good}}$ with basis $1, \alpha, \beta$ has the form

$$\begin{aligned} \alpha^2 &= -ac + b\alpha - a\beta \\ \beta^2 &= -bd + d\alpha - c\beta \\ \alpha\beta &= -ad \end{aligned}$$

for some a, b, c, d, and that conversely any a, b, c, d yield a based algebra in $\mathfrak{B}_3^{1,\mathrm{good}}$. Thus $\mathfrak{B}_3^{1,\mathrm{good}} \simeq \mathbb{A}^4$, and $\mathfrak{B}_3^1 \simeq \mathbb{A}^2 \times \mathbb{A}^4 \simeq \mathbb{A}^6$. □

Remark 5.2. In Section 8 we will find that for $n \geq 4$, the scheme $\mathfrak{B}_n^1$ is not smooth over $\operatorname{Spec}\mathbb{Z}$, so in particular it is not isomorphic to affine space.

6. The étale locus

Given $\tilde{\mathcal{A}} := (\mathcal{A}, \phi) \in \mathfrak{B}_n(S)$, we may define an $\mathcal{O}_S$-linear trace map $\operatorname{Tr}\colon \mathcal{A} \to \mathcal{O}_S$ in the usual way. Let $b_i = \phi^{-1}(e_i) \in H^0(S, \mathcal{A})$; these form an $\mathcal{O}_S$-basis of $\mathcal{A}$. Define a regular function $\Delta\colon \mathfrak{B}_n \to \mathbb{A}^1$ by setting

$$\Delta(\tilde{\mathcal{A}}) := \det\left(\operatorname{Tr}(b_i b_j)\right) \in H^0(S, \mathcal{O}_S).$$

Acting on $\tilde{\mathcal{A}}$ by $M \in \mathrm{GL}_n(S)$ multiplies the matrix in the definition of $\Delta(\tilde{\mathcal{A}})$ by $(M^{-1})^t$ on the left and M^{-1} on the right, so

$$\Delta(M \cdot \tilde{\mathcal{A}}) = (\det M)^{-2} \Delta(\tilde{\mathcal{A}}).$$

In particular, the zero locus $\{\Delta = 0\}$ and its complement $\mathfrak{B}_n^{\mathrm{et}}$ in $\mathfrak{B}_n$ are GL_n-invariant. Call the open affine subscheme $\mathfrak{B}_n^{\mathrm{et}}$ of $\mathfrak{B}_n$ the étale locus. The following is standard:

Proposition 6.1. *The following are equivalent for $\tilde{\mathcal{A}} := (\mathcal{A}, \phi) \in \mathfrak{B}_n(S)$:*

(i) $\tilde{\mathcal{A}} \in \mathfrak{B}_n^{\mathrm{et}}(S)$.
(ii) $\Delta(\tilde{\mathcal{A}}) \in H^0(S, \mathcal{O}_S^\times)$.
(iii) *The morphism* $\mathbf{Spec}\,\mathcal{A} \to S$ *is étale.*
(iv) *There exists a surjective étale base extension $f\colon T \to S$ and an isomorphism $f^*\mathcal{A} \simeq f^*\mathcal{A}_{\mathrm{split}}$.*

Examples 6.2.

(1) We have $\Delta(\tilde{\mathcal{A}}_{\mathrm{split}}) = 1$, so $\tilde{\mathcal{A}}_{\mathrm{split}} \in \mathfrak{B}_n^{\mathrm{et}}(S)$.
(2) If $n \geq 2$, $\Delta(\bullet) = 0$, so $\bullet \notin \mathfrak{B}_n^{\mathrm{et}}(S)$.

Let S_n denote the constant group scheme over $\mathbb{Z}$ corresponding to the symmetric group on n letters. Embed S_n in GL_n as the subgroup of permutation matrices.

Theorem 6.3. *There is a* GL_n*-equivariant isomorphism from the homogeneous space* GL_n / S_n *to* $\mathfrak{B}_n^{\mathrm{et}}$.

Proof. We have a morphism $\mathrm{GL}_n \to \mathfrak{B}_n^{\mathrm{et}}$ sending M to $M \cdot \tilde{\mathcal{A}}_{\mathrm{split}}$. The equivalence of (i) and (iv) in Proposition 6.1 implies that $\mathrm{GL}_n \to \mathfrak{B}_n^{\mathrm{et}}$ is surjective.

It remains to show that the subgroup scheme of GL_n stabilizing $\tilde{\mathcal{A}}_{\mathrm{split}}$ equals S_n. Equivalently, we must show that for any connected scheme S, the automorphism group of the $\mathcal{O}_S$-algebra $\prod_{i=1}^n \mathcal{O}_S$ equals S_n (acting by permuting coordinates). This holds, since every automorphism of the S-scheme $\coprod_{i=1}^n S$ induces a permutation of the connected components, and each map between components is the identity $S \to S$ by virtue of being an S-morphism. □

Corollary 6.4. *The scheme* $\mathfrak{B}_n^{\mathrm{et}}$ *is irreducible.*

Corollary 6.5. *The Zariski closure* $\overline{\mathfrak{B}_n^{\mathrm{et}}}$ *of* $\mathfrak{B}_n^{\mathrm{et}}$ *in* $\mathfrak{B}_n$ *is an irreducible component of* $\mathfrak{B}_n$.

Corollary 6.6. *The affine variety* $\mathfrak{B}_{n,k}^{\mathrm{et}}$ *is irreducible and of dimension* n^2.

Corollary 6.7. *The Zariski closure* $\overline{\mathfrak{B}_{n,k}^{\mathrm{et}}}$ *of* $\mathfrak{B}_{n,k}^{\mathrm{et}}$ *in* $\mathfrak{B}_{n,k}$ *is an irreducible component of* $\mathfrak{B}_{n,k}$ *of dimension* n^2.

Warning 6.8. Conceivably, the base extension $\left(\overline{\mathfrak{B}_n^{\mathrm{et}}}\right)_k$ could be strictly larger than $\overline{\mathfrak{B}_{n,k}^{\mathrm{et}}}$. Hence we cannot conclude that $\left(\overline{\mathfrak{B}_n^{\mathrm{et}}}\right)_k$ is irreducible.

Remark 6.9. We could similarly define $\mathfrak{B}_n^{1,\mathrm{et}}$ and prove that $\mathfrak{B}_n^{1,\mathrm{et}} \simeq H/(gS_ng^{-1})$, where g is an element of $\mathrm{GL}_n(\mathbb{Z})$ that maps $\tilde{\mathcal{A}}_{\mathrm{split}}$ to a based algebra consisting of $\mathcal{A}_{\mathrm{split}}$ with a basis whose first element is 1. The analogues of Corollaries 6.4 to 6.7 for $\mathfrak{B}_n^{1,\mathrm{et}}$ follow. In particular, $\dim \mathfrak{B}_{n,k}^{1,\mathrm{et}} = n^2 - n$.

Remark 6.10. The number of isomorphism types of rank-n algebras over an algebraically closed field k is finite if and only if $n \le 6$ [Poo08]. It follows that $\dim \mathfrak{B}_{n,k} = n^2$ and $\dim \mathfrak{B}_{n,k}^1 = n(n-1)$ for $n \le 6$, even if k is not algebraically closed. Actually, these dimension formulas hold also for $n = 7$, at least if k is of characteristic not 2 or 3, because $\mathfrak{B}_{n,k}$ is irreducible by [Maz80, Corollary 4], and hence equals $\overline{\mathfrak{B}_{n,k}^{\mathrm{et}}}$.

Remark 6.11. One might expect at first that all k-algebras are degenerations of étale algebras; i.e., that $\mathfrak{B}_{n,k}^{\mathrm{et}}$ is Zariski dense in $\mathfrak{B}_{n,k}$. In Section 9 we will disprove this for large n by proving that $\dim \mathfrak{B}_{n,k} \ge \frac{2}{27}n^3$. In fact, for every $n \ge 8$, the variety $\mathfrak{B}_{n,k}$ has irreducible components other than $\overline{\mathfrak{B}_n^{\mathrm{et}}}$: see Proposition 9.6.

7. Connectedness

Proposition 7.1. *Suppose* $n \ge 1$. *Then* $\mathfrak{B}_n^1$ *is the affine cone over a closed subscheme in a weighted projective space. The vertex of the cone is* $\bullet$.

Proof. As in the proof of Proposition 5.1, view $\mathfrak{B}_n^1$ as a closed subscheme of the $\mathbb{A}^{(n-1)^2 n}$ with coordinates c_{ij}^ℓ with $2 \le i, j \le n$ and $1 \le \ell \le n$. Let the weight of c_{ij}^ℓ be 2 if $\ell = 1$, and 1 otherwise. Then the equations expressing commutativity and associativity are homogeneous. The origin in $\mathbb{A}^{(n-1)^2 n}$ corresponds to the multiplication table for $\bullet$. □

Corollary 7.2. *The point* $\bullet \in \mathfrak{B}_n^1(k)$ *belongs to every irreducible component of* $\mathfrak{B}_{n,k}^1$.

Remark 7.3. The observation that every algebra in $\mathfrak{B}^1_{n,k}$ can be connected to $\bullet$ is due to Manjul Bhargava.

Corollary 7.4. *The point $\bullet$ belongs to every irreducible component of $\mathfrak{B}_{n,k}$.*

Proof. The inclusion $\mathfrak{B}^1_n \to \mathfrak{B}_n$ factors as

$$\mathfrak{B}^1_n \longrightarrow \mathrm{GL}_n \times \mathfrak{B}^1_n \longrightarrow \mathfrak{B}_n \tag{7.5}$$

in which the first map sends $\tilde{A}$ to $(1_n, \tilde{A})$, and the second map is a torsor under H, by Proposition 3.1. Since GL_n and H are irreducible, the base extension of (7.5) to k induces bijections on irreducible components. ☐

As a corollary, we obtain

Theorem 7.6. *The varieties $\mathfrak{B}^1_{n,k}$ and $\mathfrak{B}_{n,k}$ are connected.*

8. Smoothness

Proposition 8.1. *For $n \neq 2$, the tangent space $T_\bullet(\mathfrak{B}^1_{n,k})$ has dimension $n(n-1)^2/2$.*

Proof. By Proposition 5.1, we may assume $n \geq 3$. A deformation of $\bullet$ to a based algebra in $\mathfrak{B}^1_{n,k}(k[\epsilon]/(\epsilon^2))$ is given in terms of a basis $e_1, \ldots, e_n$ (with $e_1 = 1$) by the $\frac{n(n-1)}{2} \cdot n$ multiplication constants c^ℓ_{ij} for $2 \leq i \leq j \leq n$ and $1 \leq \ell \leq n$, in which $c^\ell_{ij} = \gamma^\ell_{ij}\epsilon$ with $\gamma^\ell_{ij} \in k$. In assuming $i \leq j$, we have already imposed commutativity, so it remains to examine the restrictions on the γ^ℓ_{ij} imposed by associativity.

The condition $(e_2e_2)e_3 = e_2(e_2e_3)$ implies $\gamma^1_{22} = 0$ and $\gamma^1_{23} = 0$. Similarly $\gamma^1_{ij} = 0$ for all i, j. No other conditions are imposed, so the dimension equals the number of (i, j, ℓ) satisfying $2 \leq i \leq j \leq n$ and $2 \leq \ell \leq n$. This is $\frac{n(n-1)}{2} \cdot (n-1)$. ☐

Corollary 8.2. *For $n \neq 2$, the tangent space $T_\bullet(\mathfrak{B}_{n,k})$ has dimension $n(n-1)^2/2 + n$.*

Proof. Using (7.5), we find $\dim T_\bullet(\mathfrak{B}_{n,k}) = \dim T_\bullet(\mathfrak{B}^1_{n,k}) + \dim \mathrm{GL}_n - \dim H$. ☐

Corollary 8.3. *For $n \geq 4$, the point $\bullet$ is singular on both $\mathfrak{B}^1_{n,k}$ and $\mathfrak{B}_{n,k}$.*

Proof. The irreducible component $\overline{\mathfrak{B}^{1,\mathrm{et}}_{n,k}}$ of $\mathfrak{B}^1_{n,k}$ contains $\bullet$ and its dimension $n(n-1)$ is less than $\dim T_\bullet(\mathfrak{B}^1_{n,k}) = n(n-1)^2/2$ if $n \geq 4$. ☐

Proposition 8.4. *For $n \in \mathbb{Z}_{\geq 0}$, the following are equivalent:*

(1) *$n \leq 3$.*
(2) *$\mathfrak{B}^1_{n,k}$ is smooth.*
(3) *$\mathfrak{B}_{n,k}$ is smooth.*

Proof. By Proposition 3.1, $\mathfrak{B}^1_{n,k}$ is smooth if and only if $\mathfrak{B}_{n,k}$ is. For $n \leq 3$ use Proposition 5.1 or Remark 4.6. For $n \geq 4$ use Corollary 8.3. ☐

Example 8.5. Let R be a discrete valuation ring with uniformizer π. Let A be the based R/π^2R-algebra with basis $1, x, y, z$ satisfying $x^2 = \pi x$, $y^2 = \pi y$, $z^2 = \pi z$, $xy = \pi z$, $yz = \pi x$, $zx = \pi y$. Then A does not lift to a free R/π^3R-algebra of rank 4, let alone a free R-algebra of rank 4: the associative relation $x^2y = x(xy)$ fails for any lift to R/π^3R. This violation of the infinitesimal lifting criterion for smoothness shows again that $\mathfrak{B}_4$ is not smooth.

9. Dimension: lower bound

Lemma 9.1. *Suppose that $n, d, r \in \mathbb{Z}_{\geq 0}$ satisfy $r \leq d(d+1)/2$ and $n = 1 + d + r$. Then*

$$\dim \mathfrak{B}_{n,k} \geq r\left(\frac{d(d+1)}{2} - r\right) + n^2 - (d^2 + dr).$$

Proof. Let $\mathfrak{m} = (x_1, \ldots, x_d) \subseteq k[x_1, \ldots, x_d]$. Then $\dim \mathfrak{m}^2/\mathfrak{m}^3 = d(d+1)/2$. Let $Z_{d,r}$ be the variety parameterizing (V, ϕ) where V is a codimension-r subspace of $\mathfrak{m}^2/\mathfrak{m}^3$, and ϕ is a k-linear isomorphism $\frac{k[x_1,\ldots,x_d]}{\mathfrak{m}^3}/V \to k^n$. The forgetful map $(V, \phi) \mapsto V$ exhibits $Z_{d,r}$ as a GL_n-torsor over the Grassmannian $\mathrm{Gr}(r, d(d+1)/2)$, so

$$\dim Z_{d,r} = \dim \mathrm{Gr}(r, d(d+1)/2) + \dim \mathrm{GL}_n = r\left(\frac{d(d+1)}{2} - r\right) + n^2.$$

We next compute the dimension of the fibers of the morphism $\pi\colon Z_{d,r} \to \mathfrak{B}_{n,k}$ defined by $(V, \phi) \mapsto (A_V, \phi)$ where $A_V := \frac{k[x_1,\ldots,x_d]}{\mathfrak{m}^3}/V$. For fixed V, to give a k-algebra isomorphism from A_V to some $A_{V'}$ is to give $(\ell, \eta_1, \ldots, \eta_d)$ where ℓ is a k-linear isomorphism $\mathfrak{m}/\mathfrak{m}^2 \to \mathfrak{m}/\mathfrak{m}^2$ such that $\mathrm{Sym}^2 \ell\colon \mathfrak{m}^2/\mathfrak{m}^3 \to \mathfrak{m}^2/\mathfrak{m}^3$ maps V to V' and $\eta_1, \ldots, \eta_d \in \frac{\mathfrak{m}^2}{\mathfrak{m}^3}/V'$. (The isomorphism $A_V \to A_{V'}$ attached to such data is given by $x_i \mapsto \ell(x_i) + \eta_i$.) It follows that given (V, ϕ), the dimension of the fiber of $Z_{d,r} \to \mathfrak{B}_{n,k}$ containing it equals the number of parameters needed to specify ℓ and $\eta_1, \ldots, \eta_d$. Thus the fibers have dimension $d^2 + dr$.

Hence

$$\dim \mathfrak{B}_{n,k} \geq \dim \pi(Z_{d,r}) = r\left(\frac{d(d+1)}{2} - r\right) + n^2 - (d^2 + dr).$$

□

Theorem 9.2. *For $n \geq 1$,*

$$\dim \mathfrak{B}_{n,k} \geq \begin{cases} \frac{2}{27}n^3 + \frac{1}{9}n^2 + \frac{5}{3}n - 1, & \text{if } n \equiv 0 \pmod 3 \\ \frac{2}{27}n^3 + \frac{1}{9}n^2 + \frac{14}{9}n - \frac{20}{27}, & \text{if } n \equiv 1 \pmod 3 \\ \frac{2}{27}n^3 + \frac{1}{9}n^2 + \frac{5}{3}n - \frac{37}{27}, & \text{if } n \equiv 2 \pmod 3. \end{cases}$$

Proof. Calculus shows that for fixed $n \geq 1$, the bound in Lemma 9.1 (with $r = n - 1 - d$) as a function of d increases up to a point around $2n/3 - 7/6 + o(1)$ and decreases thereafter. Evaluating the bound on the two integers on each side shows that the maximum at nonnegative integers occurs at $d = \lfloor \frac{2n-2}{3} \rfloor$, and the maximum value is as shown. □

Remark 9.3. The idea to use local algebras with $\mathfrak{m}^3 = 0$ to obtain a lower bound of the form $(\frac{2}{27} + o(1))n^3$ is old, but Theorem 9.2 seems to be more precise than other results of its type.

Corollary 9.4. *If $n \geq 11$, then $\dim \mathfrak{B}_{n,k} > n^2$.*

Remark 9.5. It is natural to guess that the true dimension of $\mathfrak{B}_{n,k}$ equals n^2 for $n \leq 10$, and equals the lower bound of Theorem 9.2 for $n \geq 11$.

Proposition 9.6. *If $n \geq 8$, then $\mathfrak{B}_{n,k}$ is reducible.*

Proof. It suffices to give a rank-8 algebra that cannot be deformed to an étale algebra, since then rank-n algebras with the same property can be obtained by taking a product with an étale algebra of rank $n-8$. An explicit rank-8 algebra with this property was first given in [IE78]. An example somewhat simpler than the one given there is

$$\frac{k[a,b,c,d]}{(a^2,ab,b^2,c^2,cd,d^2,ad-bc)},$$

whose construction grew out of discussions of a working group at Berkeley (Jonah Blasiak, Dustin Cartwright, David Eisenbud, Daniel Erman, Mark Haiman, the present author, Bernd Sturmfels, Mauricio Velasco, and Bianca Viray). The method for showing that a point P of $\mathfrak{B}_{n,k}$ corresponding to this algebra is not in the component $\overline{\mathfrak{B}^{\mathrm{et}}_{n,k}}$ is the same as in [IE78]: one calculates that $\dim T_P(\mathfrak{B}_{n,k}) < \dim \overline{\mathfrak{B}^{\mathrm{et}}_{n,k}} = n^2$ (or rather, one does an equivalent calculation in the Hilbert scheme). □

Proposition 9.7. *For each $n \geq 8$, there exists a prime p and an $\mathbb{F}_p$-algebra that is not isomorphic to A/pA for any order A in an étale $\mathbb{Q}$-algebra.*

Proof. We will show that any algebra coming from a point of $\mathfrak{B}_n(\mathbb{F}_p) - \overline{\mathfrak{B}^{\mathrm{et}}_n}(\mathbb{F}_p)$ has the property; the algebra

$$A_0 := \frac{\mathbb{F}_p[a,b,c,d]}{(a^2,ab,b^2,c^2,cd,d^2,ad-bc)} \times \mathbb{F}_p \times \cdots \times \mathbb{F}_p$$

from the proof of Proposition 9.6, with $n-8$ factors of $\mathbb{F}_p$, is an example.

If A is an order in an étale $\mathbb{Q}$-algebra, and we choose a $\mathbb{Z}$-basis, then the corresponding section $s\colon \operatorname{Spec}\mathbb{Z} \to \mathfrak{B}_n$ is such that $s(\operatorname{Spec}\mathbb{Q}) \in \mathfrak{B}^{\mathrm{et}}_n$, so $s(\operatorname{Spec}\mathbb{Z}) \subseteq \overline{\mathfrak{B}^{\mathrm{et}}_n}$, and $s(\operatorname{Spec}\mathbb{F}_p) \in \overline{\mathfrak{B}^{\mathrm{et}}_n}(\mathbb{F}_p)$. In other words, the point of $\mathfrak{B}_n(\mathbb{F}_p)$ corresponding to A/pA with its basis is in $\overline{\mathfrak{B}^{\mathrm{et}}_n}(\mathbb{F}_p)$, so $A/pA \not\simeq A_0$. □

Question 9.8. Can one characterize the k-algebras that correspond to points of $\overline{\mathfrak{B}^{\mathrm{et}}_{n,k}}$?

Closely related is the following:

Question 9.9. What functor does the $\mathbb{Z}$-scheme $\overline{\mathfrak{B}^{\mathrm{et}}_n}$ represent?

10. Dimension: upper bound

We now work toward an asymptotically matching upper bound on $\dim \mathfrak{B}_{n,k}$, namely $\dim \mathfrak{B}_{n,k} \leq \frac{2}{27}n^3 + O(n^{8/3})$. Such a result is announced in [Ner87], who writes that the proof is nearly identical to the proof he gives for the moduli space of n-dimensional Lie algebras. We will give details of a proof for $\mathfrak{B}_{n,k}$.

The approach towards both those results is to adapt the proof (begun in [Hig60] and completed in [Sim65]) that the number of p-groups of order p^n is $p^{\frac{2}{27}n^3+O(n^{8/3})}$. As suggested to us by Hendrik Lenstra, there is an analogy between the powers of the maximal ideal of a local finite-rank k-algebra and the descending p-central series of a p-group. Although there seems to be no direct connection between finite-rank k-algebras and finite p-groups, the combinatorial structure in the two enumeration proofs are nearly identical.

10.1. **Symmetric bilinear maps.** This subsection is inspired by [Sim65, §2], which studied alternating bilinear maps.

Throughout this subsection, we fix the following notation. Let V and W be vector spaces over a field k. Let $m = \dim V$ and $n = \dim W$. For Proposition 10.1 and its two corollaries, we fix a symmetric bilinear map $(\ ,\ )\colon V \times V \to W$. For any subspace $U \leq V$, let (U, U) be the k-span of the set $\{(u_1, u_2) : u_1, u_2 \in U\}$.

Proposition 10.1. *Suppose that $(V, V) = W$ but for no proper subspace $U \leq V$ is $(U, U) = W$. Then there exists a basis $x_1, \dots, x_m$ of V such that for $1 \leq i \leq m-1$, if V_i is the span $\langle x_1, \dots, x_i \rangle$ then $(x_i, x_{i+1}) \notin (V_i, V_i)$.*

Proof. We show by induction that for $r = 0, 1, \dots, m$ that there exist $x_1, \dots, x_r$ such that $(x_i, x_{i+1}) \notin (V_i, V_i)$ for $1 \leq i \leq r-1$. If $r \leq 1$, this is trivial. The proof of the inductive step is as in the proof of [Sim65, Proposition 2.1]. □

Corollary 10.2. *Under the hypothesis of Proposition 10.1, $m \leq n+1$.*

Corollary 10.3. *There exists a subspace $U \leq V$ such that $\dim U \leq n+1$ and $(U, U) = (V, V)$.*

Proof. Apply Corollary 10.2 to a minimal subspace U satisfying $(U, U) = (V, V)$. □

Proposition 10.4. *Suppose that k is a finite field $\mathbb{F}_q$ of order q. Let V, W, m, n be as before, and let $s \in \mathbb{Z}_{>0}$. The number of symmetric bilinear maps $(\ ,\ )\colon V \times V \to W$ such that for some s-dimensional subspace $U \leq V$ we have $(U, U) = W$, but for no $(s-1)$-dimensional subspace $U' \leq V$ is $(U', U') = W$ is less than or equal to*

$$q^{\frac{m^2}{2}(n-s)+O((m+n)^{8/3})}.$$

Proof. See the proof of [Sim65, 2.4–2.6]. The only differences are

(1) We have q instead of a prime p; this is of no consequence.
(2) Since we deal with symmetric forms in place of his alternating forms, the $\binom{m}{2}$ that appears in the proof of Sims' Proposition 2.6 should be replaced by $\binom{m+1}{2}$. Both of these are close enough to $m^2/2$ that the difference in the resulting exponent is dominated by the $O((m+n)^{8/3})$ term.

□

10.2. **Finite local $\mathbb{F}_q$-algebras.** Our next step is to count rank-n local $\mathbb{F}_q$-algebras A with residue field $\mathbb{F}_q$. Given such an A, we will define a collection of data, and then prove that the data uniquely determine A up to isomorphism.

Let $\mathfrak{m}$ be the maximal ideal of A. For $i \geq 0$, let $m_i = \dim_{\mathbb{F}_q} \mathfrak{m}^i/\mathfrak{m}^{i+1}$. Let $g_{01} = 1$. Let $V := \mathfrak{m}/\mathfrak{m}^2$ and $W := \mathfrak{m}^2/\mathfrak{m}^3$. The multiplication in A induces a symmetric bilinear map $(\ ,\ )\colon V \times V \to W$ such that $(V, V) = W$. Let $\bar{V} \leq V$ be a subspace of minimum dimension such that $(\bar{V}, \bar{V}) = W$. Let $s := \dim \bar{V}$. By Corollary 10.3, $s \leq m_2 + 1$. By Proposition 10.1, we may choose a basis $x_1, \dots, x_s$ of $\bar{V}$ such that for $i \in [1, s-1]$ we have $(x_i, x_{i+1}) \notin (V_i, V_i)$, where $V_i := \langle x_1, \dots, x_i \rangle$. For $i \in [0, s]$, let $W_i = (V_i, V_i)$ and $d_i = \dim W_i$. So $0 = d_0 \leq d_1 < d_2 < \cdots < d_s = m_2$. Choose a basis $y_1, \dots, y_{m_2}$ of W such that $W_i = \langle y_1, \dots, y_{d_i} \rangle$. Given i and $j \in (d_{i-1}, d_i]$ we may assume $y_j = (x_b, x_i)$ for some $b \in [1, i]$ depending on j. Extend $x_1, \dots, x_s$ to a basis $x_1, \dots, x_{m_1}$ of V. Choose a representative $g_{1i} \in A$ of each x_i. For each i and each $j \in (d_{i-1}, d_i]$, take $g_{2j} = g_{1b}g_{1i}$ as the representative of y_j for the same b as above. By induction on i, the map

$$\frac{\mathfrak{m}^{i-1}}{\mathfrak{m}^i} \otimes \bar{V} \to \frac{\mathfrak{m}^i}{\mathfrak{m}^{i+1}}$$

induced by multiplication in A is surjective for each $i \geq 2$. Thus in particular, by induction on i, for $i \geq 3$, we can choose $g_{i1}, \ldots, g_{i,m_i} \in A$ representing a basis of $\mathfrak{m}^i/\mathfrak{m}^{i+1}$ such that each g_{ij} equals $g_{i-1,r}g_{1\ell}$ for some $r \in [1, m_{i-1}]$ and $\ell \in [1, s]$. For $i = 3$, if X_h denotes the image of

$$\frac{\mathfrak{m}^2}{\mathfrak{m}^3} \otimes V_h \to \frac{\mathfrak{m}^3}{\mathfrak{m}^4}$$

we may assume moreover that the $g_{3j} = g_{2r}g_{1\ell}$ are chosen so that the first few have $\ell = 1$ and span X_1, and the next few have $\ell = 2$ and with the previous ones span X_2, and so on up to $\ell = s$. Then in each product $g_{2r}g_{1\ell}$ arising at the ℓ^{th} stage (i.e., mapping to $X_\ell - X_{\ell-1}$), we have $r > d_{\ell-1}$, since otherwise $g_{2r} = g_{1b}g_{1c}$ for some $b \leq c \leq \ell - 1$ and the class of $g_{2r}g_{1\ell} = g_{1b}g_{1\ell}g_{1c}$ in $\mathfrak{m}^3/\mathfrak{m}^4$ lies in $X_{\ell-1}$, and hence is not a new basis element of the ℓ^{th} stage.

The g_{ij} for $i \geq 0$ and $j \in [1, m_i]$ form a basis for A. Define $c_{ij\ell uv} \in \mathbb{F}_q$ by

$$g_{ij}g_{1\ell} = \sum c_{ij\ell uv}g_{uv}.$$

Proposition 10.5. *The isomorphism type of a local $\mathbb{F}_q$-algebra A with residue field $\mathbb{F}_q$ is determined by the sequence $(m_i)_{i\geq 0}$ and the $c_{ij\ell uv}$ for (i, j, ℓ, u, v) satisfying the following conditions:*

$i = 1$, $1 \leq j \leq \ell \leq m_1$, $u \geq 2$, $1 \leq v \leq m_u$; *or*
$i = 2$, $1 \leq \ell \leq s$, $d_{\ell-1} < j \leq m_2$, $u \geq 3$, $1 \leq v \leq m_u$; *or*
$i \geq 3$, $1 \leq j \leq m_i$, $1 \leq \ell \leq s$, $u > i$, $1 \leq v \leq m_u$;

where s and the d_i are determined by the $c_{1j\ell uv}$.

Proof. Given the data above, we construct the vector space underlying A by taking the $\mathbb{F}_q$-vector space with basis g_{ij}. Since A is generated as a $\mathbb{F}_q$-algebra by the $g_{1\ell}$ for $1 \leq \ell \leq m_1$, it suffices to show that the given data determine $g_{ij}g_{1\ell}$ for $i \geq 1$ as a linear combination of the g_{uv}.

If $i = 1$, then by commutativity we may assume $j \leq \ell$, in which case the value of $g_{1j}g_{1\ell}$ is already given by the $c_{1j\ell uv}$.

We next prove by strong induction on ℓ that $g_{2j}g_{1\ell}$ is determined for all j and all $\ell \leq s$. Suppose that the values $g_{2j}g_{1\ell'}$ have been determined for all j whenever $\ell' < \ell$, and we want to determine $g_{2j}g_{1\ell}$. If $j > d_{\ell-1}$, the relevant $c_{2j\ell uv}$ have already been given. So assume $j \leq d_{\ell-1}$. Then $g_{2j} = g_{1b}g_{1c}$ for some $b \leq c \leq \ell - 1$, so $g_{2j}g_{1\ell} = (g_{1b}g_{1\ell})g_{1c}$. Here $g_{1b}g_{1\ell}$ is a known combination of the g_{uv} for $u \geq 2$ and all v. But $g_{2v}g_{1c}$ has been determined already by the inductive hypothesis, and $g_{uv}g_{1c}$ for $u \geq 3$ is already given (since $c \leq \ell - 1 \leq s$), so the product $g_{2j}g_{1\ell} = (g_{1b}g_{1\ell})g_{1c}$ is determined.

We now know that multiplication by $g_{1\ell}$ on all the g_{ij} with $i \geq 1$ is determined provided that $\ell \leq s$. To extend this to all $\ell \leq m_1$, we use induction on i. The case $i = 1$ is already given by the known $c_{1j\ell uv}$. So assume $i \geq 2$. Then $g_{ij} = g_{i-1,r}g_{1b}$ for some r, b with $b \leq s$, so $g_{ij}g_{1\ell} = (g_{i-1,r}g_{1\ell})g_{1b}$. By the inductive hypothesis, $g_{i-1,r}g_{1\ell}$ is a known combination of g_{uv} with $u \geq 2$, so its product with g_{1b} is determined (since $b \leq s$). □

Proposition 10.6. *The number of rank-n local $\mathbb{F}_q$-algebras with residue field $\mathbb{F}_q$ is $q^{\frac{2}{27}n^3+O(n^{8/3})}$ as $n \to \infty$. The implied constant can be chosen independent of q.*

Proof. The lower bound comes from Lemma 9.1 and Theorem 9.2: using standard formulas for $\# \operatorname{Gr}(r, d(d+1)/2)(\mathbb{F}_q)$ and $\# \operatorname{GL}_n(\mathbb{F}_q)$, one obtains a lower bound that is at least a constant times q raised to the right hand side in Theorem 9.2.

Now for the upper bound. To each local $\mathbb{F}_q$-algebra A with residue field $\mathbb{F}_q$ we associate the finite list of positive integers $m_0, m_1, \ldots, m_t$ summing to n, and the $c_{ij\ell uv} \in \mathbb{F}_q$ as in Proposition 10.5. The number of possibilities for $m_0, m_1, \ldots, m_t$, including the choice of t, is at most 2^{n-1} (given n stars, place or do not place a bar between each consecutive pair of stars); this is $O(q^{n^{8/3}})$, and hence may be ignored.

Below, "log" means logarithm to the base q. The number of possibilities for s is at most $n+1$, so we may assume s is fixed. For each s, Proposition 10.4 shows that the log of the number of possibilities for the $c_{1j\ell 2v}$ giving that value of s is at most

$$\frac{m_1^2}{2}(m_2 - s) + O((m_1+m_2)^{8/3}) = \frac{m_1^2}{2}(m_2 - s) + O(n^{8/3}).$$

The log of the number of possibilities for the $c_{1j\ell uv}$ with $u \ge 3$ is $\frac{m_1(m_1+1)}{2}(n-1-m_1-m_2)$. Thus the log of the number of possibilities for all the $c_{1j\ell uv}$ is at most

$$\frac{m_1^2}{2}(n-1-m_1-s) + O(n^{8/3}).$$

The log of the number of possibilities for the $c_{2j\ell uv}$ is

$$\left(\sum_{\ell=1}^{s}(m_2 - d_{\ell-1})\right)(n-1-m_1-m_2).$$

Since $0 \le d_0 \le d_1 < d_2 < \ldots < d_s$, we have $d_{\ell-1} \ge \ell - 2$, so the value above is at most

$$\left(m_2 s - \frac{s^2}{2}\right)(n-1-m_1-m_2) + O(n^2).$$

The log of the number of possibilities for the $c_{ij\ell uv}$ for a *fixed* $i \ge 3$ is

$$m_i s(n-1-m_1-\cdots-m_i).$$

Thus the log of the number of possibilities for *all* the $c_{ij\ell uv}$ is at most

$$\frac{m_1^2}{2}(n-1-m_1-s) + \left(m_2 s - \frac{s^2}{2}\right)(n-1-m_1-m_2) + \sum_{i\ge 3} m_i s(n-1-m_1-\cdots-m_i) + O(n^{8/3}),$$

which up to $O(n^2)$ is the same as the expression M in [Sim65, p. 165]. Thus by the analysis there it is at most $\frac{2}{27}n^3 + O(n^{8/3})$. □

Proposition 10.7. *The number of rank-n local $\mathbb{F}_q$-algebras is $q^{\frac{2}{27}n^3+O(n^{8/3})}$ as $n \to \infty$. The implied constant can be chosen independent of q.*

Proof. The lower bound follows from Proposition 10.6. Each local $\mathbb{F}_q$-algebra has residue field $\mathbb{F}_{q^d}$ for some $d \mid n$, so by Proposition 10.6 their total number is

$$\sum_{d \mid n} (q^d)^{\frac{2}{27}(n/d)^3 + O((n/d)^{8/3})}.$$

This sum has at most n terms, and each is at most $q^{\frac{2}{27}n^3+O(n^{8/3})}$, so the result follows. □

10.3. **Algebras of finite rank.**

Lemma 10.8. *Suppose that $f\colon \mathbb{R}_{\geq 0} \to \mathbb{R}$ is convex and $f(0)=0$. Then $f(x_1+\cdots+x_n) \geq f(x_1)+\cdots+f(x_n)$ for any $x_1,\ldots,x_n \in \mathbb{R}_{\geq 0}$.*

Proof. This is a special case of the Hardy-Littlewood-Pólya majorization inequality [HLP88, Theorem 108], for instance. □

Theorem 10.9. *The number of rank-n $\mathbb{F}_q$-algebras is $q^{\frac{2}{27}n^3+O(n^{8/3})}$ as $n\to\infty$. The implied constant can be chosen independent of q.*

Proof. The lower bound follows from Proposition 10.7. A general $\mathbb{F}_q$-algebra is a product of local ones. Thus we may specify a rank-n $\mathbb{F}_q$-algebra by giving a partition $n=\lambda_1+\cdots+\lambda_m$ and a local $\mathbb{F}_q$-algebra A_i of rank λ_i for each i.

The number of partitions (even if we did not impose an ordering on the λ_i) is $\leq 2^{n-1} < q^{O(n^{8/3})}$, so it will suffice to bound the number of algebras for a fixed partition. By Proposition 10.7, this number is

$$\leq q^{f(\lambda_1)+\cdots+f(\lambda_m)}$$

where $f(x) := \frac{2}{27}x^3 + cx^{8/3}$ for some universal constant $c>0$. Lemma 10.8 gives the desired upper bound. □

Theorem 10.10. *We have $\dim \mathfrak{B}_{n,k} = \frac{2}{27}n^3 + O(n^{8/3})$ uniformly in k.*

Proof. We may replace k by its minimal subfield. For fixed n, $\dim \mathfrak{B}_{n,\mathbb{Q}} = \dim \mathfrak{B}_{n,\mathbb{F}_p}$ for all but finitely many primes p, so it suffices to obtain a bound for $\dim \mathfrak{B}_{n,\mathbb{F}_p}$ that is uniform in p. Theorem 10.9 estimates $\#\mathfrak{B}_{n,\mathbb{F}_p}(\mathbb{F}_{p^e})$ for every e (the latter count includes the choice of a basis, but the number of choices is only $O(p^{n^2})$). Taking $e\to\infty$ and applying the Lang-Weil bounds [LW54], we obtain the desired result. □

11. Commutative rings of finite order

As a bonus, Theorem 10.9 leads to an asymptotic formula for the number of (commutative) rings of order p^n, namely $p^{\frac{2}{27}n^3+O(n^{8/3})}$. To prove this, we follow [KP70], which proved the analogous formula $p^{\frac{4}{27}n^3+O(n^{8/3})}$ for the number of associative rings of order p^n that are not necessarily commutative or unital. We begin with the commutative analogue of [KP70, Theorem 3.1].[1]

Lemma 11.1. *The number of (commutative) rings of order p^n up to isomorphism is at most p^{n^2+n} times the number of rank-n $\mathbb{F}_p$-algebras up to isomorphism.*

Proof. ([KP70]) For each ring R of order p^n, choose generators $x_1,\ldots,x_m$ of the additive group of R such that their orders $p^{a_1},\ldots,p^{a_m}$ multiply to p^n. For $i\leq m$ and $0\leq j<a_i$, let $y_{ij}=p^jx_i$. Rename all the y_{ij} in any order as $z_1,\ldots,z_n$. Then $z_iz_j=\sum c_{ijk}z_k$ for some $c_{ijk}\in\{0,1,\ldots,p-1\}$. Construct the rank-$n$ $\mathbb{F}_p$-algebra A having the same structure

[1]Note added July 29, 2021: Simon R. Blackburn and K. Robin McLean pointed out that the argument in [KP70] is not correct, so the proof of Lemma 11.1 is not correct either. Thus the proofs of the upper bounds in Theorems 11.2 and 11.3 are not complete. The theorems are nevertheless true: they are proved (with improved error terms) in [BM21].

constants c_{ijk} considered in $\mathbb{F}_p$. Associativity, commutativity, and existence of 1 for R imply the corresponding properties for A.

The construction above defines a map from the set of isomorphism classes of rings of order p^n to the set of pairs $(\vec{a}, A)$ where $\vec{a} = (a_1, \dots, a_m)$ is a sequence of positive integers summing to n, and A is a based rank-n $\mathbb{F}_p$-algebra. Reversing the construction shows that this map is injective.

The number of sequences $\vec{a}$ is $2^{n-1} \le p^n$, and the number of choices of basis for a rank-n $\mathbb{F}_p$-algebra is $\#\operatorname{GL}_n(\mathbb{F}_p) \le p^{n^2}$. □

Theorem 11.2. *The number of commutative rings of order* p^n *up to isomorphism is* $p^{\frac{2}{27}n^3+O(n^{8/3})}$ *as* $n \to \infty$*. The implied constant can be chosen independent of* p*.*

Proof. Combine Theorem 10.9 and Lemma 11.1. □

Theorem 11.3. *The number of commutative rings of order* $\le N$ *up to isomorphism is* $\exp(\frac{2}{27}(\log N)^3/(\log 2)^2 + O((\log N)^{8/3}))$ *as* $N \to \infty$*.*

Proof. The lower bound is attained already by considering the commutative rings of order $2^{\lfloor \log_2 N \rfloor}$, by Theorem 11.2.

For the upper bound, it suffices to prove the same bound for the number r_N of commutative rings of *exact* order N, since $r_0 + \dots + r_N \le (N+1)\max_{i\in[0,N]} r_i$, and $N+1 < \exp((\log N)^{8/3})$ for large N.

By Theorem 11.2, there exists $c \ge 0$ such that the number of rings of order p^n is $\le p^{(2/27)n^3 + cn^{8/3}}$. Write $N = \prod_p N_p$, where N_p is a power of the prime p. Then

$$\begin{aligned}
\log r_N &\le \sum_{p|N} \left(\frac{2}{27}\left(\frac{\log N_p}{\log p}\right)^3 + c\left(\frac{\log N_p}{\log p}\right)^{8/3}\right)\log p \\
&\le \sum_{p|N} \left(\frac{2}{27}\frac{(\log N_p)^3}{(\log 2)^2} + c\frac{(\log N_p)^{8/3}}{(\log 2)^{5/3}}\right) \\
&\le \frac{2}{27}\frac{(\log N)^3}{(\log 2)^2} + c\frac{(\log N)^{8/3}}{(\log 2)^{5/3}},
\end{aligned}$$

by Lemma 10.8. □

The main contribution to the number of finite rings may come from those of the form $(\frac{\mathbb{Z}_2[[x_1,\dots,x_d]]}{\mathfrak{m}^3})/V$ where $\mathbb{Z}_2$ is the ring of 2-adic integers, $\mathfrak{m} = (2, x_1, \dots, x_d)$, and V is an $\mathbb{F}_2$-subspace of $\mathfrak{m}^2/\mathfrak{m}^3$. If this is so, then we would obtain the following information about the "typical" finite ring:

Conjecture 11.4. As $N \to \infty$, the fraction of (isomorphism classes of) commutative rings A of order $\le N$ satisfying the following conditions tends to 1:

(1) The size of A is 2^n, where 2^n is the largest power of 2 less than or equal to N.
(2) The ring A is local.
(3) The residue field of A is $\mathbb{F}_2$.
(4) If $\mathfrak{m}$ is the maximal ideal of A, then $\mathfrak{m}^3 = 0$ but $\mathfrak{m}^2 \ne 0$.
(5) The $\mathbb{F}_2$-dimension of $\mathfrak{m}/\mathfrak{m}^2$ is $2n/3 + O(1)$.
(6) The characteristic of A is 8 (i.e., we have $8 = 0$ but $4 \ne 0$ in A).

Similar questions have been raised for groups: see [Man99], for instance.

12. Hilbert schemes revisited

Finally, we use the results and techniques in Sections 9 and 10 to estimate the dimension of $\mathrm{Hilb}_n(\mathbb{A}^d)$ when d is at least about as large as n.

Corollary 12.1. *If $d \geq n-1$,*

$$\dim \mathrm{Hilb}_n(\mathbb{A}^d)_k = \frac{2}{27}n^3 + nd + O(n^{8/3}).$$

Proof. Substitute Theorem 10.10 in Corollary 4.4. □

We may generalize Corollary 12.1 to cover a larger range of d.

Theorem 12.2. *Suppose that $d = \alpha n$ for some nonnegative $\alpha \in \mathbb{Q}$. Set*

$$c_\alpha := \begin{cases} 2/27, & \text{if } \alpha \geq 2/3 \\ \frac{\alpha^2}{2}(1-\alpha) & \text{if } 0 \leq \alpha \leq 2/3. \end{cases}$$

Then for $\alpha \geq 1/2$,

$$\dim \mathrm{Hilb}_n(\mathbb{A}^d)_k = c_\alpha n^3 + nd + O(n^{8/3}).$$

For $\alpha < 1/2$, we have only the inequality

$$\dim \mathrm{Hilb}_n(\mathbb{A}^d)_k \geq c_\alpha n^3 + O(n^2).$$

Proof. Let $\mathfrak{B}_{n,k,d}$ be the image of $\mathfrak{H}_n(\mathbb{A}^d)_k \to \mathfrak{B}_{n,k}$, so $\mathfrak{B}_{n,k,d}$ parameterizes rank-n algebras that can be generated by d elements. By Corollary 4.2, $\mathfrak{B}_{n,k,d}$ is open in $\mathfrak{B}_{n,k}$. The proof of Corollary 4.4 generalizes to show that

$$\dim \mathrm{Hilb}_n(\mathbb{A}^d)_k = \dim \mathfrak{B}_{n,k,d} - n^2 + nd,$$

so it suffices to estimate $\dim \mathfrak{B}_{n,k,d}$.

For $d \geq 2n/3$, we still have

$$\dim \mathfrak{B}_{n,k,d} = \frac{2}{27}n^3 + O(n^{8/3}),$$

since the algebras constructed in Lemma 9.1 for the lower bound on $\dim \mathfrak{B}_{n,k}$ in Theorem 9.2 could be generated by about $2n/3$ elements.

For $d = \alpha n$ with $\alpha < 2/3$, we can use Lemma 9.1 to obtain

$$\dim \mathfrak{B}_{n,k,d} \geq c_\alpha n^3 - O(n^2).$$

If $1/2 \leq \alpha \leq 2/3$, we obtain a matching upper bound (but with error term $O(n^{8/3})$) by generalizing the proof of Theorem 10.10 as follows. Proceed as in the proof of Proposition 10.6, but at the end impose the additional condition that $m_1 \leq \alpha n$. This translates, in the notation of [Sim65, p. 165], into the constraint $x \leq \alpha$ in addition to the constraints $x + y \leq 1$, $0 \leq y \leq x$. The constant in front of the n^3 in the lower bound obtained is the maximum value of

$$B(x,y) := x^2(1-x-y)/2 + y^2(1-x-y)/2 + y(1-x-y)^2/2$$

subject to these constraints. For fixed $x \geq 1/2$, calculus shows that the maximum value of $B(x,y)$ for $y \in [0, 1-x]$ occurs at $y = 0$, and the value there is $\frac{x^2}{2}(1-x) = c_x$. Calculus shows also that the maximum value of $B(x,y)$ on the triangle with vertices $(0,0)$, $(1/2,0)$, $(1/2,1/2)$ is attained at $(1/2,0)$. By the previous two sentences, for $1/2 \leq \alpha \leq 2/3$, the maximum value of $B(x,y)$ on the region defined by $x \le \alpha$ in addition to the constraints $x+y \le 1$, $0 \le y \le x$ is $\frac{\alpha^2}{2}(1-\alpha)$, attained at $(\alpha, 0)$. □

Remark 12.3. Before the present work, it seems that asymptotic bounds for $\dim \operatorname{Hilb}_n(\mathbb{A}^d)_k$ were known only as $n \to \infty$ for fixed d: it is shown in [BI78] that this dimension is bounded above and below by universal positive constants times $n^{2-2/d}$.

Acknowledgements

I thank Hendrik Lenstra for the insight that enumeration of finite-rank algebras might be related to enumeration of p-groups. I thank also Manjul Bhargava, Bas Edixhoven, Mark Haiman, and David Helm for discussions, and I thank the referee for several helpful suggestions. I thank Andrew O'Desky for a correction in Remark 6.9. This work was begun at the trimester on "Explicit methods in number theory" at the Institut Henri Poincaré in 2004, and continued at U. C. Berkeley and at the workshop on "Rings of low rank" at the Lorentz Center in 2006. The author's research is supported partially by NSF grant DMS-0301280.

References

[Bha04a] Manjul Bhargava, *Higher composition laws. I. A new view on Gauss composition, and quadratic generalizations*, Ann. of Math. (2) **159** (2004), no. 1, 217–250. MR2051392 (2005f:11062a) ↑1.2

[Bha04b] ———, *Higher composition laws. II. On cubic analogues of Gauss composition*, Ann. of Math. (2) **159** (2004), no. 2, 865–886. MR2081442 (2005f:11062b) ↑1.2

[Bha04c] ———, *Higher composition laws. III. The parametrization of quartic rings*, Ann. of Math. (2) **159** (2004), no. 3, 1329–1360. MR2113024 (2005k:11214) ↑1.2

[Bha05] ———, *The density of discriminants of quartic rings and fields*, Ann. of Math. (2) **162** (2005), no. 2, 1031–1063. MR2183288 ↑1.2

[BM21] Simon R. Blackburn and K. Robin McLean, *Enumerating finite rings*, July 28, 2021. Preprint, `arXiv:2107.13215v1`. ↑1

[BI78] J. Briançon and A. Iarrobino, *Dimension of the punctual Hilbert scheme*, J. Algebra **55** (1978), no. 2, 536–544. MR523473 (80g:14013) ↑12.3

[DF40] B. N. Delone and D. K. Faddeev, *Theory of Irrationalities of Third Degree*, Acad. Sci. URSS. Trav. Inst. Math. Stekloff, vol. 11, 1940 (Russian); English transl., *The theory of irrationalities of the third degree*, Translations of Mathematical Monographs, vol. 10, Amer. Math. Soc., Providence, RI, 1964. MR0004269 (2,349d) ↑5

[Fla68] F. J. Flanigan, *Algebraic geography: Varieties of structure constants*, Pacific J. Math. **27** (1968), 71–79. MR0237573 (38 #5854) ↑1.2

[Fog68] John Fogarty, *Algebraic families on an algebraic surface*, Amer. J. Math **90** (1968), 511–521. MR0237496 (38 #5778) ↑4.6

[Gab74] Peter Gabriel, *Finite representation type is open*, Algebras (Carleton Univ., Ottawa, Ont., 1974), Carleton Univ., Ottawa, Ont., 1974, pp. 23 pp. Carleton Math. Lecture Notes, No. 9. MR0376769 (51 #12944) ↑1.2

[GGS02] Wee Teck Gan, Benedict Gross, and Gordan Savin, *Fourier coefficients of modular forms on G_2*, Duke Math. J. **115** (2002), no. 1, 105–169. MR1932327 (2004a:11036) ↑5

[HLP88] G. H. Hardy, J. E. Littlewood, and G. Pólya, *Inequalities*, Cambridge Mathematical Library, Cambridge University Press, Cambridge, 1988. Reprint of the 1952 edition. MR944909 (89d:26016) ↑10.3

[Hig60] Graham Higman, *Enumerating p-groups. I. Inequalities*, Proc. London Math. Soc. (3) **10** (1960), 24–30. MR0113948 (22 #4779) ↑10

[Iar87] A. Iarrobino, *Hilbert scheme of points: overview of last ten years*, Algebraic geometry, Bowdoin, 1985 (Brunswick, Maine, 1985), Proc. Sympos. Pure Math., vol. 46, Amer. Math. Soc., Providence, RI, 1987, pp. 297–320. MR927986 (89b:14007) ↑1.2

[IE78] A. Iarrobino and J. Emsalem, *Some zero-dimensional generic singularities; finite algebras having small tangent space*, Compositio Math. **36** (1978), no. 2, 145–188. MR515043 (81c:14004) ↑9

[KP70] Robert L. Kruse and David T. Price, *Enumerating finite rings*, J. London Math. Soc. (2) **2** (1970), 149–159. MR0251079 (40 #4310) ↑11, 11, 1

[LW54] Serge Lang and André Weil, *Number of points of varieties in finite fields*, Amer. J. Math. **76** (1954), 819–827. MR0065218 (16,398d) ↑10.3

[LBR99] Lieven Le Bruyn and Zinovy Reichstein, *Smoothness in algebraic geography*, Proc. London Math. Soc. (3) **79** (1999), no. 1, 158–190. MR1687535 (2000d:16018) ↑1.2

[Man99] Avinoam Mann, *Some questions about p-groups*, J. Austral. Math. Soc. Ser. A **67** (1999), no. 3, 356–379. MR1716701 (2000k:20051) ↑11

[Maz79] Guerino Mazzola, *The algebraic and geometric classification of associative algebras of dimension five*, Manuscripta Math. **27** (1979), no. 1, 81–101. MR524979 (81g:16039) ↑1.2

[Maz80] ———, *Generic finite schemes and Hochschild cocycles*, Comment. Math. Helv. **55** (1980), no. 2, 267–293. MR576606 (82k:14010) ↑1.2, 6.10

[Maz82] ———, *How to count the number of irreducible components of the schemes of finite-dimensional algebra structures*, J. Algebra **78** (1982), no. 2, 292–302. MR680361 (84d:16039) ↑1.2

[Ner87] Yu. A. Neretin, *An estimate for the number of parameters defining an n-dimensional algebra*, Izv. Akad. Nauk SSSR Ser. Mat. **51** (1987), no. 2, 306–318, 447 (Russian); English transl., Math. USSR-Izv. **30** (1988), no. 2, 283–294. MR896999 (88i:17001) ↑1.2, 10

[Poo08] Bjorn Poonen, *Isomorphism types of commutative algebras of finite rank over an algebraically closed field*, Computational arithmetic geometry, Contemp. Math., vol. 463, Amer. Math. Soc., Providence, RI, 2008, pp. 111–120, DOI 10.1090/conm/463/09050. MR2459993 (2010c:13018) ↑1.3, 6.10

[Sim65] Charles C. Sims, *Enumerating p-groups*, Proc. London Math. Soc. (3) **15** (1965), 151–166. MR0169921 (30 #164) ↑10, 10.1, 10.1, 10.1, 10.2, 12

Department of Mathematics, University of California, Berkeley, CA 94720-3840, USA
Email address: poonen@math.berkeley.edu
URL: http://math.berkeley.edu/~poonen/