

The unit theorem for finite-dimensional algebras

Hendrik Lenstra

Notes for a mini-course given at the Max Planck Institute for Mathematics in Bonn, on October 25th and November 3rd 2016.

Summary. The *unit theorem* to which the present mini-course is devoted is a theorem from algebra that has a combinatorial flavour, and that originated in fact from algebraic combinatorics. Beyond a proof, the course also addresses applications, one of which is a proof of the normal basis theorem from Galois theory.

1.	Introduction	1
2.	The combinatorial Nullstellensatz	6
3.	The Jacobson radical	10
4.	Proof of the unit theorem	13
5.	Descending module properties	16
6.	Glynn's determinant formula	20
7.	A lower bound and an algorithm	22
8.	References	25

1. Introduction

An *algebra* over a commutative ring F is a ring A equipped with a ring homomorphism $F \rightarrow Z(A) = (\text{center of } A)$ (so that the multiplication map $A \times A \rightarrow A$ is F -bilinear). Let F be a field. An algebra A over F is called *finite-dimensional* if the dimension of A , viewed as a vector space over F , is finite.

Theorem (Unit theorem). *Let F be a field, let A be a finite-dimensional algebra over F , and let H be an additive subgroup of A that spans A as an F -vector space. Then H contains a unit of A .*

If H is as in the theorem, then H contains some *basis* B for A as a vector space over F , and H will then also contain the additive subgroup of A generated by B ; that additive subgroup equals $\sum_{b \in B} (\mathbf{Z} \cdot 1) \cdot b$, where $\mathbf{Z} \cdot 1$ denotes the prime subring of F (so $\mathbf{Z} \cdot 1 \cong \mathbf{Z}/(\text{char } F)\mathbf{Z}$). Conversely, if B is any F -vector space basis for A , then $\sum_{b \in B} (\mathbf{Z} \cdot 1) \cdot b$ is an additive subgroup of A that spans A as an F -vector space. So we see that the unit theorem is equivalent to the following statement: if A is a finite-dimensional algebra over a field F , with vector space basis B , then A contains a unit all of whose coefficients on B belong to the prime subring of F .

Exercise 1. Show that the theorem is incorrect without the finite dimensionality assumption.

Interesting examples of finite-dimensional algebras over F are: matrix rings over F ; group rings of finite groups over F ; extension fields of finite degree over F (for which the unit theorem is trivial); and rings of the form $F^n = F \times F \times \dots \times F$ (n copies of F , for some $n \in \mathbf{Z}_{\geq 0}$), with componentwise ring operations. Algebras of the latter type are said to be *totally split*. For a totally split algebra, the unit theorem says: if B is a basis for F^n over F , then some *integral* linear combination of B has all coordinates different from zero.

The three main subjects of the present mini-course are a *proof* of the unit theorem, *applications*, and the case of *commutative* algebras.

The proof. To explain the main idea and the main difficulty of the proof, I give it in a special case. Let F and A be as in the unit theorem. As we saw above, we may assume that H is the additive subgroup of A generated by some vector space basis b_1, b_2, \dots, b_n of A over F . For $x = \sum_{i=1}^n x_i b_i \in A$ (with $x_i \in F$), let $M(x)$ be the $n \times n$ -matrix that describes the F -linear map $A \rightarrow A$, $a \mapsto xa$, on the basis b_1, b_2, \dots, b_n . Then x is a unit of A if and only if $\det M(x) \neq 0$.

Also, one has $M(x) = \sum_{i=1}^n x_i M(b_i)$, so if one defines the element P of the polynomial ring $F[X_1, \dots, X_n]$ by

$$P = \det \left(\sum_{i=1}^n X_i M(b_i) \right)$$

then one has $\det M(x) = P(x_1, x_2, \dots, x_n)$, and x is a unit of A if and only if $P(x_1, x_2, \dots, x_n) \neq 0$. Since for $x = 1$ one has $\det M(x) = 1 \neq 0$, the polynomial P is not the zero polynomial. Now make the assumption that F has *characteristic zero* or, equivalently, that its prime subring is infinite. We may identify that prime subring with \mathbf{Z} . Since, by a well-known theorem (see §2), a non-zero polynomial in n variables over a field does not vanish identically on any product of n infinite subsets of the field, there exists $(x_1, x_2, \dots, x_n) \in \mathbf{Z} \times \mathbf{Z} \times \dots \times \mathbf{Z}$ with $P(x_1, x_2, \dots, x_n) \neq 0$. This gives rise to an element $x = \sum_{i=1}^n x_i b_i$ that belongs to H and is a unit, as desired.

This proves the unit theorem in the case of characteristic *zero*. In the case of non-zero characteristic p , the main difficulty is that a non-zero polynomial may vanish identically on a product of finite sets, such as $\mathbf{Z}/p\mathbf{Z} \times \mathbf{Z}/p\mathbf{Z} \times \dots \times \mathbf{Z}/p\mathbf{Z}$. To overcome this difficulty, we shall develop a variant of the *combinatorial Nullstellensatz* that is independent of the choice of coordinates; it states that, under certain conditions, the phenomenon just described does not occur. To prove that in our case those conditions are satisfied, we use a classical structure theorem for finite-dimensional algebras over an algebraically closed field.

Exercise 2. Let F, A, H be as in the unit theorem, and assume that F has characteristic zero. Prove that every coset $a + H$ of H , with $a \in A$, contains a unit of A .

Applications. To illustrate the applications of the unit theorem, we use it to obtain a mild sharpening of the *normal basis theorem* from Galois theory. Let $E \subset F$ be a finite Galois extension of fields, with Galois group G . It is well-known that one has $\#G = [F : E]$. The normal basis theorem asserts that there exists $\alpha \in F$ such that $(\sigma\alpha)_{\sigma \in G}$ is a basis for F as a vector space over E . We shall prove the following.

Theorem. *Let E, F, G be as above, and let H be an additive subgroup of F that spans F as an E -vector space. Then there exists $\alpha \in H$ such that $(\sigma\alpha)_{\sigma \in G}$ is a vector space basis of F over E .*

Exercise 3. Verify this theorem directly in the case $E = \mathbf{R}, F = \mathbf{C}$.

To deduce the theorem from the unit theorem, we let $F[G]$ denote the group ring of G over F , and we define $\varphi: F \rightarrow F[G]$ by

$$\varphi(\alpha) = \sum_{\tau \in G} (\tau^{-1}\alpha) \cdot \tau.$$

This map has the following properties:

- (i) φ is E -linear,
- (ii) $\varphi(\sigma\alpha) = \sigma \cdot \varphi(\alpha)$ for all $\sigma \in G, \alpha \in F$,
- (iii) for any basis $(b_i)_{i \in I}$ for F as an E -vector space, $(\varphi(b_i))_{i \in I}$ is a basis for $F[G]$ as an F -vector space.

Here (i) is obvious, and (ii) follows from an easy computation. For (iii), it suffices to show that the square matrix $(\tau b_i)_{\tau \in G, i \in I}$ is invertible. Suppose $a_\tau \in F$, for $\tau \in G$, are such that for all $i \in I$ one has $\sum_{\tau \in G} a_\tau \tau b_i = 0$. Then for all $b \in F$ one has $\sum_{\tau \in G} a_\tau \tau b = 0$, so by Artin's theorem on linear independence of field homomorphisms one has $a_\tau = 0$ for all $\tau \in G$, and (iii) follows.

Now let H be as in the theorem. Then H spans F as an E -vector space, so (iii) shows that $\varphi(H)$ spans $F[G]$ as an F -vector space. Applying the unit theorem, with $F[G]$ and $\varphi(H)$ in the roles of A and H , we can choose $\alpha \in H$ such that $\varphi(\alpha)$ is a unit of $F[G]$. Then $F[G] \cdot \varphi(\alpha) = F[G]$, so $(\sigma \cdot \varphi(\alpha))_{\sigma \in G}$ is linearly independent over F . Hence (ii) shows that $(\varphi(\sigma\alpha))_{\sigma \in G}$ is linearly independent over F , so *a fortiori* over E . From (i) it now follows that $(\sigma\alpha)_{\sigma \in G}$ is linearly independent over E , so it is a basis for F over E , as required.

Exercise 4. Let E, F, G, φ be as above.

- (a) Prove that φ is a ring homomorphism if and only if $E = F$.
- (b) Let $\alpha \in F$. Prove: $(\sigma\alpha)_{\sigma \in G}$ is a basis for F over E if and only if $\varphi(\alpha)$ is a unit of $F[G]$.

The normal basis theorem is equivalent to the assertion that F , when viewed as a module over the group ring $E[G]$, is isomorphic to $E[G]$ itself. Paraphrasing the proof just given, one may say that it starts by verifying this assertion “after base extension from E to F ”; more precisely, the properties of φ show that there is an isomorphism $F \otimes_E F \cong E[G] \otimes_E F$ of modules over the ring $E[G] \otimes_E F$, which is nothing but the group ring $F[G]$. Next, the unit theorem is used to “descend” this isomorphism from F to E . All applications of the unit theorem that we shall give, are to similar *descent problems*.

The commutative case. In the commutative case, we start with the following exercise, in which R^* denotes the group of units of a ring R .

Exercise 5. Let A be a commutative finite-dimensional algebra over some field F . Prove that for some $n \in \mathbf{Z}_{\geq 0}$ there exists a vector space isomorphism $\psi: F^n \rightarrow A$ such that $\psi(F^{*n}) \subset A^*$.

This exercise shows that, in order to prove the unit theorem in the case A is commutative, one may assume that A is *totally split*, in which case, as we saw above, the unit theorem allows a reformulation that does not refer to the ring structure.

In the commutative case, the unit theorem admits several different proofs, each of which supplies additional information. For example, we have the following result, which I learnt from Bas Edixhoven.

Theorem. *Let F, A, H be as in the unit theorem, and write n for the dimension of A as an F -vector space. Assume that the characteristic p of F is non-zero, and that A is commutative. Then the number of units of A contained in H is at least $(p - 1)^n$.*

One may wonder whether the theorem remains true without the commutativity assumption.

2. The combinatorial Nullstellensatz

Throughout this section, F denotes a field. For a non-zero polynomial g in several variables, we write $\deg g$ for the total degree of g .

In the introduction we used the well-known fact that if $g \in F[X_1, \dots, X_n]$ is non-zero, with $n \in \mathbf{Z}_{\geq 0}$, and S_1, S_2, \dots, S_n are infinite subsets of F , then g does not vanish identically on $S_1 \times S_2 \times \dots \times S_n$. The *combinatorial Nullstellensatz* is a quantitative refinement of this statement.

Theorem (Combinatorial Nullstellensatz, Noga Alon, 1999). *Let F be a field, let $n \in \mathbf{Z}_{\geq 0}$, $d_1, d_2, \dots, d_n \in \mathbf{Z}_{\geq 0}$, and let $g \in F[X_1, \dots, X_n]$. Suppose that g has a non-zero coefficient at $X_1^{d_1} \cdots X_n^{d_n}$ and that $d_1 + d_2 + \dots + d_n = \deg g$. Let $S_i \subset F$ satisfy $\#S_i > d_i$, for $1 \leq i \leq n$. Then g does not vanish identically on $S_1 \times \dots \times S_n$.*

Proof. For $x = (x_1, x_2, \dots, x_n) \in F^n$ the map $F[X_1, \dots, X_n] \rightarrow F$, $f \mapsto f(x) = f(x_1, x_2, \dots, x_n)$ is a surjective ring homomorphism, so denoting its kernel by $I(x)$, we have $F[X_1, \dots, X_n]/I(x) \cong F$. We have

$$I(x) + I(y) = F[X_1, \dots, X_n] \text{ for } x = (x_j)_{j=1}^n, y = (y_j)_{j=1}^n \in F^n, x \neq y,$$

since if $x_j \neq y_j$ then $I(x) + I(y)$ contains $(X_j - x_j) - (X_j - y_j) = y_j - x_j$, which is a unit. The Chinese remainder theorem now implies that, for any finite subset $S \subset F^n$, the map

$$F[X_1, \dots, X_n] \rightarrow \prod_{x \in S} F[X_1, \dots, X_n]/I(x) \cong F^S$$

sending $f \in F[X_1, \dots, X_n]$ to $(f(x))_{x \in S}$ in F^S , is a *surjective* ring homomorphism.

Turning to the proof of the theorem, we assume, without loss of generality, that each S_i is *finite* of cardinality $d_i + 1$, and we apply the above to $S =$

$S_1 \times S_2 \times \dots \times S_n$. For each i , the polynomial

$$h_i = \prod_{x \in S_i} (X_i - x)$$

is a monic polynomial in X_i of degree $d_i + 1$, and it belongs to the kernel of the ring homomorphism $F[X_1, X_2, \dots, X_n] \rightarrow F^S$ that we defined. We claim that this ring homomorphism is still surjective when restricted to the F -vector space V (say) spanned by

$$X_1^{i_1} X_2^{i_2} \cdots X_n^{i_n} \text{ with all } i_j \in \{0, 1, \dots, d_j\}.$$

To see this, it suffices to observe that for each $f \in F[X_1, X_2, \dots, X_n]$ one can perform successive “divisions with remainder” by h_1, h_2, \dots, h_n to find $r(f) \in V$ with $f \equiv r(f) \pmod{(h_1, h_2, \dots, h_n)}$, so that f and $r(f)$ have the same image in F^S .

The hypothesis $d_1 + d_2 + \dots + d_n = \deg g$ ensures that g and $r(g)$ have the same coefficient at $X_1^{d_1} \cdots X_n^{d_n}$. Since it was supposed to be non-zero, it follows that $r(g) \neq 0$.

Because V and F^S both have F -dimension $\prod_{j=1}^n (d_j + 1)$, the surjective map $V \rightarrow F^S$, which is F -linear, is actually an isomorphism of F -vector spaces. Hence $r(g)$ does not map to 0. It follows that g does not map to $0 \in F^S$, which is the statement to be proved. This proves the combinatorial Nullstellensatz.

Exercise 6. Prove that, in the situation of the proof just given, the kernel of the surjective ring homomorphism $F[X_1, \dots, X_n] \rightarrow F^S$ is for $S = S_1 \times S_2 \times \dots \times S_n$ generated by h_1, h_2, \dots, h_n . *Can you also prove that for *any* finite subset $S \subset F^n$ the kernel can be generated by n elements?

Exercise 7. Prove that the combinatorial Nullstellensatz remains valid if the conditions on g are replaced by the following: g has a non-zero term $cX_1^{d_1} \cdots X_n^{d_n}$ (with $c \in F$) such that no other non-zero term $c'X_1^{e_1} \cdots X_n^{e_n}$ (with $c' \in F$) of g satisfies $e_1 \geq d_1, \dots, e_n \geq d_n$.

The combinatorial Nullstellensatz has seen many dramatic applications in extremal graph theory and in arithmetic combinatorics. As an example of the

latter type, we give a quick proof of the *theorem of Cauchy–Davenport*. It has seen many proofs through the ages, but none is as brief as the present one.

Theorem (Cauchy, 1813; Davenport, 1935). *Let p be a prime number, let $A, B \subset \mathbf{Z}/p\mathbf{Z}$ be non-empty subsets, and put $A + B = \{a + b : a \in A, b \in B\}$. Then we have $\#(A + B) \geq \min\{\#A + \#B - 1, p\}$.*

Proof. If $\#A + \#B > p$, then for each $c \in \mathbf{Z}/p\mathbf{Z}$ the sets A and $c - B$ must intersect, and therefore $A + B = \mathbf{Z}/p\mathbf{Z}$. Assume therefore that $\#A + \#B \leq p$. If the claim fails, then we can choose $C \subset \mathbf{Z}/p\mathbf{Z}$ with $A + B \subset C$ and $\#C = \#A + \#B - 2$. Then $g = \prod_{c \in C} (X_1 + X_2 - c)$ vanishes on $A \times B$, has degree $\#A + \#B - 2$, and has a non-zero coefficient at $X_1^{\#A-1} \cdot X_2^{\#B-1}$, contradicting the combinatorial Nullstellensatz. This proves the theorem.

We next prove that, in a special case, the set of $g \in F[X_1, \dots, X_n]$ to which the combinatorial Nullstellensatz applies, is invariant under invertible linear substitutions of X_1, \dots, X_n .

Lemma. *Suppose that the characteristic p of the field F is non-zero, and let $m, n \in \mathbf{Z}_{\geq 0}$. Denote by G the group of ring automorphisms of $F[X_1, \dots, X_n]$ that are the identity on F and that map $F \cdot X_1 + \dots + F \cdot X_n$ to itself, and write \mathfrak{D} for the set of all $g \in F[X_1, \dots, X_n]$ that have a non-zero term $cX_1^{d_1} \dots X_n^{d_n}$ (with $c \in F$) satisfying*

$$d_i < p^m \text{ for all } i, \text{ and } \sum_{i=1}^n d_i = \deg g.$$

Then for all $\sigma \in G$ we have $\sigma\mathfrak{D} = \mathfrak{D}$.

Note that \mathfrak{D} consists of those polynomials that by the combinatorial Nullstellensatz are guaranteed *not* to vanish identically on any set of the form $S_1 \times S_2 \times \dots \times S_n$, where each $S_i \subset F$ satisfies $\#S_i = p^m$.

Proof of the lemma. For $g \in F[X_1, \dots, X_n]$, we write $\text{lt } g$ for the sum of the terms of degree $\deg g$ of g if $g \neq 0$, and $\text{lt } 0 = 0$. We have $g \notin \mathfrak{D}$ if and only if

every term of $\text{lt } g$ is for some j divisible by $X_j^{p^m}$. In other words, writing I for the ideal $(X_1^{p^m}, \dots, X_n^{p^m})$ of $F[X_1, \dots, X_n]$, we have

$$g \notin \mathfrak{D} \iff \text{lt } g \in I.$$

Let $\sigma \in G$, and put $V = F \cdot X_1 + \dots + F \cdot X_n$. Since the map $v \mapsto v^{p^m}$ is additive, I is the same as the ideal generated by $\{v^{p^m} : v \in V\}$. Thus, from $\sigma V = V$ it follows that $\sigma I = I$. It also follows that σ preserves degree and homogeneity of polynomials, and therefore that $\text{lt } \sigma(g) = \sigma(\text{lt } g)$. Thus we have

$$g \notin \mathfrak{D} \iff \text{lt } g \in I \iff \sigma(\text{lt } g) \in \sigma I \iff \text{lt}(\sigma g) \in I \iff \sigma g \notin \mathfrak{D}.$$

This implies the lemma.

Exercise 8. Let $F, p, m, n, G, \mathfrak{D}$ be as in the lemma.

- (a) Prove: G is isomorphic to the group $\text{GL}(n, F)$ of invertible $n \times n$ -matrices over F .
- (b) Let Γ be the group of all ring automorphisms σ of $F[X_1, \dots, X_n]$ with the property that $\deg(\sigma g) = \deg g$ for all non-zero $g \in F[X_1, \dots, X_n]$. Prove: for all $\sigma \in \Gamma$ one has $\sigma \mathfrak{D} = \mathfrak{D}$.
- (c) Prove that the group Γ from (b) is isomorphic to a repeated semidirect product $F^n \rtimes (\text{GL}(n, F) \rtimes \text{Aut } F)$.

Theorem (p -power non-vanishing theorem). *Let F be a field of non-zero characteristic p , let $m, n \in \mathbf{Z}_{\geq 0}$, $d_1, d_2, \dots, d_n \in \mathbf{Z}_{\geq 0}$, and suppose $d_i < p^m$ for all i . Let $g \in F[X_1, \dots, X_n]$ be a polynomial with $\deg g = d_1 + d_2 + \dots + d_n$ that has a non-zero coefficient at $X_1^{d_1} \dots X_n^{d_n}$. Let $S_i \subset F$ satisfy $\#S_i = p^m$, for $1 \leq i \leq n$, and let b_1, b_2, \dots, b_n be a basis for the F -vector space F^n . Then g does not vanish identically on $\sum_{i=1}^n S_i b_i = \{\sum_{i=1}^n x_i b_i : x_i \in S_i \ (1 \leq i \leq n)\}$.*

Proof. Write $b_i = (b_{ij})_{j=1}^n$. Then the matrix $(b_{ij})_{i,j=1}^n$ belongs to $\text{GL}(n, F)$, and the map

$$f \mapsto \sigma f = f \left(\sum_i X_i b_{i1}, \dots, \sum_i X_i b_{in} \right)$$

is a ring automorphism σ of $F[X_1, \dots, X_n]$ that belongs to the group G defined in the lemma. With \mathfrak{D} as in the lemma, we have $g \in \mathfrak{D}$, so by the lemma we

have $\sigma g \in \mathfrak{D}$. By the combinatorial Nullstellensatz, there are $x_i \in S_i$ (for $1 \leq i \leq n$) with $(\sigma g)(x_1, \dots, x_n) \neq 0$. But

$$(\sigma g)(x_1, \dots, x_n) = g\left(\sum_i x_i b_{i1}, \dots, \sum_i x_i b_{in}\right) = g\left(\sum_i x_i b_i\right),$$

and the theorem follows.

Theorem (Non-vanishing on subgroups). *Let F be a field of non-zero characteristic p , let $n \in \mathbf{Z}_{\geq 0}$, and let $g \in F[X_1, \dots, X_n]$. Suppose that there exist integers $d_1, \dots, d_n \in \{0, 1, \dots, p-1\}$ such that $\deg g = d_1 + d_2 + \dots + d_n$ and such that g has a non-zero coefficient at $X_1^{d_1} \cdots X_n^{d_n}$. Then g does not vanish identically on any additive subgroup H of F^n that spans F^n as a vector space over F .*

Proof. It suffices to apply the previous theorem to $m = 1$, taking all S_i to be the prime field \mathbf{F}_p of F , and letting b_1, b_2, \dots, b_n be a basis for F^n that is contained in H . This proves the theorem.

Exercise 9. Prove the following characteristic zero version of the previous theorem. Let F be a field of characteristic zero, let $n \in \mathbf{Z}_{\geq 0}$, and let $g \in F[X_1, \dots, X_n]$ be non-zero. Then g does not vanish identically on any additive subgroup H of F^n that spans F^n as a vector space over F .

Exercise 10. Let k be a finite field, let $F \supset k$ be a field extension, let $n \in \mathbf{Z}_{\geq 0}$, and let $g \in F[X_1, \dots, X_n]$. Suppose that there exist integers $d_1, \dots, d_n \in \{0, 1, \dots, \#k - 1\}$ such that $\deg g = d_1 + d_2 + \dots + d_n$ and such that g has a non-zero coefficient at $X_1^{d_1} \cdots X_n^{d_n}$. Prove that g does not vanish identically on any sub- k -vector space of F^n that spans F^n as an F -vector space.

3. The Jacobson radical

The present section is devoted to two properties of the Jacobson radical that are used in our proof of the unit theorem.

Let A be a ring. We write A^* for the group of units of A . By an A -module, we shall always mean a left A -module. An A -module M is called *simple* if it

has exactly two submodules (namely, $\{0\}$ and M). The *Jacobson radical* of A is

$$J(A) = \{a \in A : aM = 0 \text{ for each simple } A\text{-module } M\}.$$

It is clearly a two-sided ideal of A .

Proposition. *Let A be a ring, and $a \in A$. Then:*

$$a \in A^* \iff a + J(A) \in (A/J(A))^*.$$

Proof. The implication \Rightarrow is clear. For \Leftarrow , define $U = \{a \in A : a + J(A) \in (A/J(A))^*\}$, and let $a \in U$. Then $Aa + J(A) = A$. If $Aa \neq A$, then A has a maximal left ideal I with $Aa \subset I$; for any such I , the module A/I is simple, so $J(A) \cdot (A/I) = 0$, and therefore $J(A) \subset I$, which leads to the contradiction $A = Aa + J(A) \subset I$. This proves $Aa = A$, so we can choose $b \in A$ with $ba = 1$. Then $b + J(A)$ is the inverse of $a + J(A)$ in the group $(A/J(A))^*$, so $b \in U$. Therefore every element of U has a left inverse in U , which implies that U is a group under multiplication, so $U \subset A^*$. This proves the proposition.

Exercise 11. Let A be a ring.

- (a) Let I be a two-sided ideal of A . Prove: $I \subset J(A) \iff 1 + I \subset A^*$.
- (b) The ring A^{opp} opposite to A has the same additive group as A , but the product of two elements x and y in A^{opp} is defined to be the product of y and x in A . Prove: $J(A^{\text{opp}}) = J(A)$.

We call a ring D a *division ring* if $D^* = D \setminus \{0\}$. By a *division algebra* over a commutative ring we mean an algebra that is a division ring. For a ring D and $m \in \mathbf{Z}_{\geq 0}$, we write $M(m, D)$ for the ring of $m \times m$ -matrices with entries in D .

Theorem. *Let F be a field, and let A be a finite-dimensional algebra over F . Then for some $t \in \mathbf{Z}_{\geq 0}$ there exist positive integers m_1, \dots, m_t and finite-dimensional division algebras D_1, \dots, D_t over F such that*

$$A/J(A) \cong \prod_{i=1}^t M(m_i, D_i)$$

as F -algebras.

Proof. We start by proving that, as an A -module, $A/\mathcal{J}(A)$ is the direct sum of a finite collection of simple A -modules. To this end, define \mathfrak{J} to be the set of those left ideals I of A for which A/I can be written as such a direct sum; for example, one has $A \in \mathfrak{J}$. Since A and all of its left ideals are finite-dimensional F -vector spaces, we can choose $I \in \mathfrak{J}$ minimal under inclusion. We claim $I = \mathcal{J}(A)$. Write $A/I = \bigoplus_{M \in \mathfrak{S}} M$, where \mathfrak{S} is a finite set of simple A -modules. Since $\mathcal{J}(A) \cdot M = 0$ for each $M \in \mathfrak{S}$, we have $\mathcal{J}(A) \cdot (A/I) = 0$, so $\mathcal{J}(A) \subset I$. Assume, for a contradiction, that the opposite inclusion is not valid. Then we can choose a simple A -module N and $x \in N$ such that $Ix \neq 0$. By simplicity of N , we have $Ix = N$, so the A -linear map $f: A \rightarrow (A/I) \oplus N$, $f(a) = (a + I, ax)$, fits in a commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & I & \longrightarrow & A & \longrightarrow & A/I & \longrightarrow & 0 \\ & & \downarrow & & \downarrow f & & \downarrow \text{id} & & \\ 0 & \longrightarrow & N & \longrightarrow & (A/I) \oplus N & \longrightarrow & A/I & \longrightarrow & 0 \end{array}$$

of A -modules that has exact rows and in which the first vertical arrow is surjective. Then f is surjective as well, from which it follows that $\ker f \in \mathfrak{J}$; but $\ker f$ is properly contained in I , so this contradicts the minimality of I . This proves our claim $I = \mathcal{J}(A)$, so $\mathcal{J}(A) \in \mathfrak{J}$, and therefore $A/\mathcal{J}(A) = \bigoplus_{M \in \mathfrak{S}} M$ for some finite set \mathfrak{S} of simple A -modules.

We now describe the endomorphism ring $\text{End}_A(A/\mathcal{J}(A))$ of the A -module $A/\mathcal{J}(A)$ in two ways. On the one hand, since $A/\mathcal{J}(A)$ is a ring, the A -linear maps $A/\mathcal{J}(A) \rightarrow A/\mathcal{J}(A)$ coincide with the right multiplications $x \mapsto xa$ by ring elements $a \in A/\mathcal{J}(A)$. Thus, in the notation of Exercise 11(b), we obtain an isomorphism $\text{End}_A(A/\mathcal{J}(A)) \cong (A/\mathcal{J}(A))^{\text{opp}}$ of F -algebras.

On the other hand, the additive group of $\text{End}_A(A/\mathcal{J}(A))$ may be identified with

$$\text{Hom}_A\left(\bigoplus_{N \in \mathfrak{S}} N, \bigoplus_{M \in \mathfrak{S}} M\right) \cong \bigoplus_{M, N \in \mathfrak{S}} \text{Hom}_A(N, M),$$

and one readily checks that the product in $\text{End}_A(A/J(A))$ is, in terms of $\bigoplus_{M,N} \text{Hom}_A(N, M)$, simply given by matrix multiplication. If $f: N \rightarrow M$ is a non-zero A -linear map, with $N, M \in \mathfrak{S}$, then by $\ker f \neq N$ and $fN \neq 0$ and simplicity we have $\ker f = 0$ and $fN = M$, so f is an *isomorphism*. Hence $\text{Hom}_A(N, M) = 0$ if $N \not\cong M$, and $\text{Hom}_A(M, M) = \text{End}_A(M)$ is a division algebra; it is finite-dimensional over F , since M is. Now if we sort the $M \in \mathfrak{S}$ by isomorphism, and let t be the number of isomorphism classes occurring, we have $\bigoplus_{M \in \mathfrak{S}} M \cong \bigoplus_{i=1}^t M_i^{m_i}$ for certain $m_i \in \mathbf{Z}_{>0}$, with endomorphism ring isomorphic to $\prod_{i=1}^t M(m_i, \text{End}_A(M_i))$ as an F -algebra.

Comparing the two descriptions of $\text{End}_A(A/J(A))$, we obtain an isomorphism

$$A/J(A) \cong \left(\prod_{i=1}^t M(m_i, \text{End}_A(M_i)) \right)^{\text{opp}} \cong \prod_{i=1}^t M(m_i, D_i)$$

of F -algebras, where $D_i = \text{End}_A(M_i)^{\text{opp}}$ and where the second isomorphism is given by transposition of matrices.

This proves the theorem.

Remark. If F is algebraically closed, then the D_i occurring in the theorem are necessarily equal to F , because every finite-dimensional division algebra D over F can be written as a union $\bigcup_{a \in D} F(a)$; each $F(a)$ is commutative, so is a finite field extension of F , and therefore equal to F itself.

4. Proof of the unit theorem

Lemma. *Let F be an algebraically closed field, and let A be a finite-dimensional algebra over F . Then there exist, for some index set J , a basis $(b_i)_{i \in J}$ for A as an F -vector space and a polynomial $g \in F[X_i : i \in J]$ such that:*

- (a) *if $x = \sum_{i \in J} x_i b_i \in A$, with each $x_i \in F$, then x is a unit of A if and only if $g((x_i)_{i \in J}) \neq 0$;*
- (b) *there exists $m \in \mathbf{Z}_{\geq 0}$ such that each non-zero term of g is of the form $\pm \prod_{i \in I} X_i$ for some subset $I \subset J$ with $\#I = m$.*

Proof. First suppose that A equals the $m \times m$ -matrix algebra over F , for some $m \in \mathbf{Z}_{>0}$. For $i, j \in \{1, \dots, m\}$, let $b_{ij} \in A$ be the matrix with (i, j) -entry 1 and all other entries 0. Then $(b_{ij})_{i,j=1}^m$ is a basis for A over F . Also, for $x_{ij} \in F$ and $x = \sum_{i,j} x_{ij} b_{ij}$, we have $x \in A^* \iff \det((x_{ij})_{i,j=1}^m) \neq 0$, so we can take $g = \det((X_{ij})_{i,j=1}^m)$; it is well known that each non-zero term of g has the form $\pm \prod_{i=1}^m X_{i\sigma(i)}$ for some permutation σ of $\{1, 2, \dots, m\}$.

Next suppose that $A = A' \times A''$ for certain F -algebras A' and A'' for which the assertion of the lemma is valid, with bases $(b'_i)_{i \in J'}$ and $(b''_i)_{i \in J''}$ and polynomials g', g'' . We may assume that J' and J'' are disjoint. Since $A^* = A'^* \times A''^*$, we may now take the basis for A to be the union of $((b'_i, 0))_{i \in J'}$ and $((0, b''_i))_{i \in J''}$, with polynomial $g = g' \cdot g''$.

We pass to the general case. Write $J(A)$ for the Jacobson radical of A . By the theorem of §3 and the remark following that theorem, the F -algebra $A/J(A)$ is isomorphic to a product of finitely many matrix algebras over F . Hence, by the cases already proved, the lemma is valid for $A/J(A)$, so there are a basis $(b_i + J(A))_{i \in J'}$ of $A/J(A)$ over F and a polynomial $g' \in F[X_i : i \in J']$ satisfying the analogues of (a) and (b). Supplementing $(b_i)_{i \in J'}$ with an F -basis for $J(A)$ we obtain a basis $(b_i)_{i \in J}$ for A over F , with $J' \subset J$. By the proposition of §3, we can now simply take $g = g'$, viewed as an element of $F[X_i : i \in J]$. This proves the lemma.

Exercise 12. Let the notation and the hypotheses be as in the lemma. Also, let \mathfrak{S} be a set of simple A -modules such that every simple A -module is isomorphic to exactly one member of \mathfrak{S} .

- (a) Prove that, when $(b_i)_{i \in J}$ and g are constructed as in the proof given, the number m in (b) is given by $m = \sum_{M \in \mathfrak{S}} \dim_F M$.
- (b) (For readers who know Hilbert's Nullstellensatz.) Prove that, whenever $(b_i)_{i \in J}$ and g satisfy (a) and (b) of the lemma, the number m in (b) is necessarily equal to $\sum_{M \in \mathfrak{S}} \dim_F M$.

We can now prove the unit theorem from the introduction, which reads as follows.

Theorem. *Let F be a field, let A be a finite-dimensional algebra over F , and let H be an additive subgroup of A that spans A as an F -vector space. Then*

H contains a unit of A .

Proof. We proved the theorem already in the introduction if $\text{char } F = 0$, so we may assume $\text{char } F = p > 0$.

Let it first be assumed that F is algebraically closed. Choose $(b_i)_{i \in J}$ and g as in the lemma. Since A^* is non-empty, part (a) of the lemma implies $g \neq 0$. By part (b), we can choose a non-zero term $\pm \prod_{i \in J} X_i^{d_i}$ of g with $\sum_i d_i = \deg g$ and all $d_i \in \{0, 1\}$. The non-vanishing theorem on subgroups, from §2, now shows that g does not vanish identically on H , so by part (a) of the lemma we have $H \cap A^* \neq \emptyset$, as required.

We pass to the general case. Let Ω be any algebraically closed field extension of F , and write A_Ω for the Ω -algebra $A \otimes_F \Omega$. We may identify A with the sub- F -algebra $A \otimes 1$ of A_Ω . As an Ω -vector space, A_Ω is spanned by A , and therefore also by H . We claim that we have $A^* = A \cap A_\Omega^*$. Namely, if $a \in A$, then one has $a \in A^*$ if and only if the matrix that describes the F -linear map $A \rightarrow A$, $x \mapsto xa$, on some F -basis for A is invertible; but this matrix doesn't change if we use the same basis for A_Ω over Ω , so its invertibility is also equivalent to $a \in A_\Omega^*$, as required.

We can now apply the case already proved to A_Ω , and find that $H \cap A_\Omega^*$ is non-empty; but $H \subset A$, so we have $H \cap A^* = H \cap A \cap A_\Omega^* = H \cap A_\Omega^* \neq \emptyset$.

This proves the unit theorem.

Exercise 13. Let F be a *perfect* field of characteristic $p > 0$, let A be a finite-dimensional algebra over F , and put $n = \dim_F A$. Prove that for every basis $(b_i)_{i=1}^n$ of A over F there exists a polynomial $g \in F[X_1, \dots, X_n]$ that satisfies the hypothesis of the non-vanishing theorem on subgroups from §2, such that for any $x = \sum_{i=1}^n x_i b_i \in A$, with $x_i \in F$, one has: $x \in A^* \iff g(x_1, \dots, x_n) \neq 0$.

Exercise 14. Let F be a field, let A be a finite-dimensional algebra over F , and let H be an additive subgroup of A that spans A as an F -vector space. Prove that every coset of H in A contains a unit of A .

Exercise 15. Let F be a field, let $m \in \mathbf{Z}_{>0}$, and let H be an additive subgroup of the ring $M(m, F)$ of $m \times m$ -matrices over F that spans $M(m, F)$ as an F -vector space. Prove that for every $c \in F$ and every $a \in M(m, F)$ there exists $x \in a + H$ with $\det x \neq c$.

5. Descending module properties

Throughout this section we make the following assumptions. By F we denote a field, and K is an extension field of F . For any F -vector space V , we shall write $V_K = V \otimes_F K$, which is a K -vector space with $\dim_K(V_K) = \dim_F(V)$; we shall always identify V with its image $V \otimes 1$ in V_K . We shall constantly use that a sequence $V \rightarrow V' \rightarrow V''$ of F -vector spaces is exact if and only if the sequence $V_K \rightarrow V'_K \rightarrow V''_K$ of K -vector spaces it induces is exact; this is because K is F -free of non-zero rank. In particular, one has $V = 0 \iff V_K = 0$, and an F -linear map $V \rightarrow V'$ is zero, injective, surjective, or bijective, if and only if the induced K -linear map $V_K \rightarrow V'_K$ has the same respective property.

By A we denote an F -algebra. Then A_K is a K -algebra and if M is an A -module, then M_K is an A_K -module. **Modules denoted by M or N will always be assumed to be finite-dimensional as vector spaces over F ;** then M_K and N_K have the same property over K . We do *not* assume that A be finite-dimensional over F ; however, when dealing with an A -module M , we can typically reduce to that case by replacing A by its image in $\text{End}_F(M)$, which does have finite F -dimension.

In the present section we are interested in properties of an A -module M that are *base-change invariant* in the sense that they pass to the induced A_K -module M_K . Each such property gives rise to a *descent problem*: if the A_K -module M_K has the property, does the same hold for the A -module M ? In many cases where the answer is affirmative, an easy proof can be given by means of the unit theorem; often a slightly sharper statement can be obtained, as was the case with the normal basis theorem in §1.

The following lemma will be constantly used.

Lemma. *Let M, N be A -modules. Then the natural map*

$$\text{Hom}_A(M, N)_K \longrightarrow \text{Hom}_{A_K}(M_K, N_K)$$

is an isomorphism.

Proof. Replacing A by its image in $(\text{End}_F M) \times \text{End}_F N$, we may assume $\dim_F(A) < \infty$. For $M = A$, both groups in the lemma may be identified with N_K , and the assertion is easy to check. For general M , we can now use a finite presentation $A^m \rightarrow A^n \rightarrow M \rightarrow 0$ of M as an A -module, and left exactness of Hom , to reduce to the previous case. This proves the lemma.

The first property we consider is *cyclicity*. We call an A -module M *cyclic* if there exists $x \in M$ with $M = Ax$ or, equivalently, if there is a surjective A -linear map $A \rightarrow M$.

Theorem (Generator theorem). *Let M be a cyclic A -module, and let H be an additive subgroup of M that spans M as an F -vector space. Then there exists $x \in H$ with $M = Ax$.*

Proof. As above, we reduce to the case $\dim_F A < \infty$. Let $f: A \rightarrow M$ be a surjective A -linear map. Then $f^{-1}H$ is an additive subgroup of A that spans A as an F -vector space, so by the unit theorem there is a unit $u \in f^{-1}H$. Then $x = f(u) \in M$ satisfies $Ax = f(Au) = f(A) = M$, as required. This proves the theorem.

Remark. See Exercise 18 for a generalization to modules that require more generators.

Theorem (Descending cyclicity). *Let M be an A -module. Then M is cyclic if and only if M_K is a cyclic A_K -module, and one has $A \cong M$ as A -modules if and only if $A_K \cong M_K$ as A_K -modules.*

Proof. Both “only if” statements are clear. For the first “if” statement, assume that M_K is a cyclic A_K -module. Applying the generator theorem, with $M_K, A_K, K, M = M \otimes 1$ in the roles of M, A, F, H , we find $x \in M$ such that the map $A \rightarrow M, a \mapsto ax$, becomes surjective after tensoring with K . Then it is already surjective, as required. For the second “if” statement, the map

$A \rightarrow M$ obtained in the same way is also injective, because $A_K \cong M_K$ implies $\dim_F A = \dim_K(A_K) = \dim_K(M_K) = \dim_F M$. This proves the theorem.

Changing rings, we can extend the second part of the theorem above to more general isomorphisms.

Theorem (Descending isomorphisms). *Let M, N be A -modules. Then one has $M \cong_A N \iff M_K \cong_{A_K} N_K$.*

Proof. It suffices to prove \Leftarrow . Let $f: M_K \rightarrow N_K$ be an A_K -linear isomorphism. Then $\text{End}_{A_K}(N_K) \rightarrow \text{Hom}_{A_K}(M_K, N_K)$, $g \mapsto gf$, is an isomorphism of $\text{End}_{A_K}(N_K)$ -modules, so by the lemma the $\text{End}_A(N)$ -module $\text{Hom}_A(M, N)$ becomes isomorphic to $\text{End}_A(N)$ after tensoring with K . Applying the theorem proved above, with $\text{End}_A N$ and $\text{Hom}_A(M, N)$ in the roles of A and M , one finds $\text{End}_A N \cong \text{Hom}_A(M, N)$ as $\text{End}_A N$ -modules, so $\text{Hom}_A(M, N) = (\text{End}_A N) \cdot h$ for some A -linear map $h: M \rightarrow N$. Then one also has $\text{Hom}_{A_K}(M_K, N_K) = \text{End}_{A_K}(N_K) \cdot h_K$ (for $h_K = h \otimes \text{id}_K$), so $f = i \cdot h_K$ for some $i \in \text{End}_{A_K}(N_K)$. Since f is an isomorphism h_K is injective, and comparing dimensions one finds that h_K is an isomorphism. Then h is an isomorphism, as desired.

Exercise 16. Suppose that M and N are isomorphic A -modules. Let H be a subgroup of $\text{Hom}_A(M, N)$ that spans $\text{Hom}_A(M, N)$ as an F -vector space. Prove that H contains an isomorphism $M \rightarrow N$ of A -modules.

Theorem (Noether–Deuring). *Let M and N be A -modules. Then there exists an A -module P with $M \cong N \oplus P$ as A -modules if and only if there exists an A_K -module Q with $M_K \cong N_K \oplus Q$ as A_K -modules.*

Proof. For the “only if”-part one can take $Q = P_K$. For the “if”-part, we write $V = \text{Hom}_A(M, N)$ and $W = \text{Hom}_A(N, M)$. Note that by the lemma, we may identify V_K with $\text{Hom}_{A_K}(M_K, N_K)$ and W_K with $\text{Hom}_{A_K}(N_K, M_K)$. Likewise, if we write $B = \text{End}_A(N)$, which is a finite-dimensional algebra over F , then we may identify B_K with $\text{End}_{A_K} N_K$. It is an easy exercise to show

that the existence of P as in the theorem is equivalent to the existence of a pair $(f, g) \in V \times W$ with $f \cdot g \in B^*$. So, to prove the theorem, it suffices to prove that such a pair exists if we are given a pair $(f', g') \in V_K \times W_K$ with $f' \cdot g' \in B_K^*$. The K -span of the subgroup $V \cdot g' \subset B_K$ equals $V_K \cdot g'$, which is a left B_K -ideal containing the unit $f' \cdot g'$ and is therefore equal to B_K . Hence, applying the unit theorem with $K, B_K, V \cdot g'$ in the respective roles of F, A, H , we find $f \in V$ with $f \cdot g' \in B_K^*$. Next, the K -span of $f \cdot W \subset B_K$ is a right B_K -ideal containing the unit $f \cdot g'$, so it equals B_K , and with $K, B_K, f \cdot W$ in the roles of F, A, H we find $g \in W$ with $f \cdot g \in B_K^*$. Since also $f \cdot g \in B$, we have $f \cdot g \in B^*$, as desired. This proves the theorem.

In the exercises that follow, the assumptions stated at the beginning of this section remain in force. This applies in particular to the assumption $\dim_F M < \infty$. We recall that a module P over a ring R is called *projective* if for any surjective R -linear map $V \rightarrow W$ of R -modules the induced map $\text{Hom}_R(P, V) \rightarrow \text{Hom}_R(P, W)$ of abelian groups is surjective; equivalently, P is projective if and only if there exists an R -module Q such that $P \oplus Q$ is a *free* R -module.

Exercise 17. Let R be a ring, let P be a projective R -module, and let V be an R -module. Prove that the following two assertions are equivalent:

- (i) there is a surjective R -linear map $f: P \rightarrow V$;
- (ii) there exists $f \in \text{Hom}_R(P, V)$ with $f \cdot \text{End}_R P = \text{Hom}_R(P, V)$, and every such f is surjective.

Exercise 18. Let $n \in \mathbf{Z}_{\geq 0}$, and let M be an A -module that can be generated by n elements. Prove that for every additive subgroup $H \subset M^n$ that spans M^n as an F -vector space there exists $(x_1, x_2, \dots, x_n) \in H$ such that $M = \sum_{i=1}^n Ax_i$.

Exercise 19. Let M be an A -module, and let P be a finitely generated projective A -module. Prove: there exists a surjective A -linear map $P \rightarrow M$ if and only if there exists a surjective A_K -linear map $P_K \rightarrow M_K$.

Exercise 20. Let M be an A -module. Prove that the least number of generators of M as an A -module is equal to the least number of generators of M_K as an A_K -module.

Exercise 21. Suppose that F is a *finite* field, let V be a 2-dimensional F -vector space, and write \mathcal{P} for the set of 1-dimensional subspaces of V .

- (a) Put $A = F \oplus F^{\mathcal{P}}$, and define a multiplication on A by $(a, x) \cdot (b, y) = (ab, ay + bx)$. Prove that A is a commutative ring and that the map $F \rightarrow A, a \mapsto (a, 0)$ is a ring homomorphism that makes A into a finite-dimensional algebra over F .
- (b) Put $M = V \oplus \bigoplus_{W \in \mathcal{P}} (V/W)$. Prove that the scalar multiplication $\cdot : A \times M \rightarrow M, (a, (b_W)_{W \in \mathcal{P}}) \cdot (x, (y_W + W)_{W \in \mathcal{P}}) = (ax, (ay_W + b_W x + W)_{W \in \mathcal{P}})$ makes M into an A -module satisfying $\dim_F M < \infty$.
- (c) Prove: there exists an injective A_K -linear map $A_K \rightarrow M_K$ if and only if $K \neq F$.

Remark. Since A is projective as an A -module, Exercise 21(c) shows that Exercise 19 may fail when injective instead of surjective maps are considered. The following exercise shows that Exercise 19 also becomes incorrect when the projectivity condition is omitted.

Exercise 22. Let F, A be as in Exercise 21. Construct A -modules P and M , both finite-dimensional over F , such that there exists a surjective A_K -linear map $P_K \rightarrow M_K$ if and only if $K \neq F$.

6. Glynn's determinant formula

In the present section we give a new proof of the commutative case of the unit theorem. Throughout this section, p is a prime number, F is a field of characteristic p , and $n \in \mathbf{Z}_{\geq 0}$.

Theorem (Glynn's determinant formula, 1998). *For any $n \times n$ -matrix $A = (a_{ij})_{i,j=1}^n$ over F , the coefficient of the polynomial*

$$\prod_{j=1}^n \left(\sum_{i=1}^n a_{ij} X_i \right)^{p-1} \quad \text{at } X_1^{p-1} X_2^{p-1} \cdots X_n^{p-1}$$

equals $(\det A)^{p-1}$.

Example. If A is a *diagonal* matrix, then an easy computation shows that one has in fact

$$\prod_{j=1}^n \left(\sum_{i=1}^n a_{ij} X_i \right)^{p-1} = (\det A)^{p-1} \cdot X_1^{p-1} \cdots X_n^{p-1}.$$

Proof of the theorem. Write V for the F -vector space $\sum_{i=1}^n F \cdot X_i$. Then $F[X_1, X_2, \dots, X_n]$ may be identified with the symmetric algebra of V over F .

Hence the group $\text{Aut } V$, which may be identified with $\text{GL}(n, F)$, acts on the F -algebra $F[X_1, X_2, \dots, X_n]$ in a natural way. Write I for the ideal generated by $\{v^p : v \in V\}$. Then for all $\sigma \in \text{Aut } V$ one has $\sigma I = I$. Also, since p -th powering is additive, the ideal I is generated by $\{X_1^p, \dots, X_n^p\}$ and has therefore as an F -basis the set of monomials $X_1^{d_1} \cdots X_n^{d_n}$ in which at least one d_i is at least p . It follows that the F -algebra $R = F[X_1, \dots, X_n]/I$ has the images of the monomials $X_1^{d_1} \cdots X_n^{d_n}$ with all $d_i < p$ as an F -basis. Hence R contains V , and the R -ideal $J = \{r \in R : rV = 0\}$ is the one-dimensional F -vector space generated by the image of $X_1^{p-1} \cdots X_n^{p-1}$ in R .

The natural action of $\text{Aut } V$ on R preserves J so yields a group homomorphism $\varphi: \text{Aut } V \rightarrow \text{Aut}_F J \cong F^*$. The latter group is abelian, so $\ker \varphi$ contains the commutator subgroup $[\text{Aut } V, \text{Aut } V]$. But if $\#F > 2$ —which we may assume, upon replacing F by a suitable extension—then by Exercise 23 we have $[\text{Aut } V, \text{Aut } V] = \ker \det$, where $\det: \text{Aut } V \rightarrow F^*$ is the determinant map. Therefore, for $\sigma \in \text{Aut } V$, the image $\varphi(\sigma)$ depends only on $\det \sigma$, and checking the case that σ is given by a diagonal matrix, one finds $\varphi(\sigma) = (\det \sigma)^{p-1}$. Rewriting this in terms of the X_i , one obtains from this Glynn's formula in the case A is invertible. In the generic case, when the a_{ij} are n^2 polynomial variables over \mathbf{F}_p and $F = \mathbf{F}_p(a_{ij} : 1 \leq i, j \leq n)$, the matrix is indeed invertible; and the general case follows from the generic case. This proves the theorem.

Exercise 23. Prove: if V is an n -dimensional vector space over F , then $[\text{Aut } V, \text{Aut } V]$ equals the kernel of $\det: \text{Aut } V \rightarrow F^*$, except in the case $n = \#F = 2$, in which case $[\text{Aut } V, \text{Aut } V]$ has index 2 in $\ker \det$.

Exercise 24. Let $m \in \mathbf{Z}_{\geq 0}$. Prove that Glynn's determinant formula is also valid when one replaces $p - 1$, at all occurrences, by $p^m - 1$.

Exercise 25. Let k be a finite field, and $d_1, d_2, \dots, d_n \in \mathbf{Z}_{\geq 0}$. Prove:

$$\sum_{x_1, x_2, \dots, x_n \in k} x_1^{d_1} \cdots x_n^{d_n} = \begin{cases} (-1)^n & \text{if each } d_i \text{ is a positive multiple of } \#k - 1, \\ 0 & \text{otherwise.} \end{cases}$$

Theorem. Let $B = \{(b_{ij})_{j=1}^n : 1 \leq i \leq n\}$ be a basis of the F -vector space F^n , and let $H \subset F^n$ be the additive subgroup generated by B . Then we have

$$\sum_{(y_1, y_2, \dots, y_n) \in H} y_1^{p-1} y_2^{p-1} \cdots y_n^{p-1} = (-1)^n \cdot (\det(b_{ij})_{i,j=1}^n)^{p-1}.$$

Proof. If we write $f = \prod_{j=1}^n (\sum_{i=1}^n b_{ij} X_i)^{p-1}$, then the sum on the left equals

$$\sum_{x_1, x_2, \dots, x_n \in \mathbf{F}_p} f(x_1, \dots, x_n)^{p-1}.$$

We apply Exercise 25 to $k = \mathbf{F}_p$. Since f is homogeneous of degree $n \cdot (p-1)$, it has at most one non-zero monomial $c \cdot X_1^{d_1} \cdots X_n^{d_n}$ with all $d_i \in \mathbf{Z}_{>0} \cdot (p-1)$, namely with all $d_i = p-1$; and the coefficient c at that monomial equals $(\det(b_{ij})_{i,j=1}^n)^{p-1}$, by Glynn's formula. Hence the theorem follows from Exercise 25. This proves the theorem.

Since the right hand side in the formula just proved is non-zero, it implies that at least one $(y_1, y_2, \dots, y_n) \in H$ satisfies $y_1 y_2 \cdots y_n \neq 0$. As we saw in section 1, this implies the commutative case of the unit theorem.

Exercise 26. Let $B = \{(b_{ij})_{j=1}^n : 1 \leq i \leq n\}$ be a basis of the F -vector space F^n , and let k be a finite subfield of F . Write W for the k -vector space generated by B . Prove:

$$\sum_{(y_1, y_2, \dots, y_n) \in W} y_1^{\#k-1} y_2^{\#k-1} \cdots y_n^{\#k-1} = (-1)^n \cdot (\det(b_{ij})_{i,j=1}^n)^{\#k-1}.$$

7. A lower bound and an algorithm

We give a third proof of the unit theorem in the commutative case, again concentrating on totally split algebras. It will lead to a lower bound, as stated in the theorem at the end of the introduction.

Throughout this section, F is a field.

Theorem. Let E be a subfield of F , and $n \in \mathbf{Z}_{\geq 0}$. Let $W \subset F^n$ be a sub- E -vector space of F^n such that the natural map $W \otimes_E F \rightarrow F^n$ is an isomorphism. Then W has a basis B over E such that $\sum_{b \in B} E^* \cdot b \subset F^{*n}$.

Proof. In this proof, we abbreviate $- \otimes_E F$ to $-_F$. For $i \in \{1, 2, \dots, n\}$, let $\pi_i: W_F \rightarrow F$ be the composition of the isomorphism $W_F \xrightarrow{\sim} F^n$ and the i -th coordinate projection $F^n \rightarrow F$. Then $W_F \rightarrow F^n$, $x \mapsto (\pi_i(x))_{i=1}^n$, is an isomorphism of F -vector spaces, which is the same as saying that $\pi_1, \pi_2, \dots, \pi_n$ form a basis for the F -vector space $\text{Hom}_F(W_F, F)$ or, equivalently, that $\pi_1 \wedge \pi_2 \wedge \dots \wedge \pi_n$ is a non-zero element of the exterior power $\bigwedge^n \text{Hom}_F(W_F, F)$, which is a 1-dimensional F -vector space.

For each i , define $W_i = W \cap (\ker \pi_i)$. The natural map $\text{Hom}_E(W/W_i, E)_F \rightarrow \text{Hom}_F(W_F/(W_i)_F, F)$ is an isomorphism (cf. the lemma in section 5). Here we may identify $\text{Hom}_F(W_F/(W_i)_F, F)$ with the set of all $f \in \text{Hom}_F(W_F, F)$ that are 0 on $(W_i)_F$; so $\pi_i \in \text{Hom}_F(W_F/(W_i)_F, F)$. The image of the natural map

$$\left(\bigotimes_{i=1}^n \text{Hom}_E(W/W_i, E) \right)_F \xrightarrow{\sim} \bigotimes_{i=1}^n \text{Hom}_F(W_F/(W_i)_F, F) \rightarrow \bigwedge^n \text{Hom}_F(W_F, F)$$

contains the non-zero element $\pi_1 \wedge \pi_2 \wedge \dots \wedge \pi_n$. It follows that there are $\rho_i \in \text{Hom}_E(W/W_i, E)$ such that the image of $\rho_1 \otimes \rho_2 \otimes \dots \otimes \rho_n$ is non-zero. Then $\rho_1 \wedge \rho_2 \wedge \dots \wedge \rho_n$ is non-zero as an element of $\bigwedge^n \text{Hom}_E(W, E)$, so the E -linear map $W \rightarrow E^n$, $x \mapsto (\rho_i(x))_{i=1}^n$, is an isomorphism. We now choose B to be the inverse image of the standard basis of E^n . Then for each $x \in \sum_{b \in B} E^* \cdot b$ and each i one has $\rho_i(x) \neq 0$, so $x \notin W_i = W \cap \ker \pi_i$, so $\pi_i(x) \neq 0$; and therefore $x \in F^{*n}$. This proves the theorem.

Theorem (Lower bound). *Let F be a field, let A be a commutative algebra over F of finite vector space dimension n , and let $H \subset A$ be an additive subgroup that spans A as an F -vector space. Assume that the characteristic p of F is positive. Then $\#(H \cap A^*) \geq (p-1)^n$.*

Proof. As we argued in the introduction, we may assume that A is totally split, so $A \cong F^n$ as F -algebras, and that H is the \mathbf{F}_p -span of some F -basis for A . With $E = \mathbf{F}_p$ and $W = H$ we can now apply the previous theorem, and we find an \mathbf{F}_p -basis B for H such that $\sum_{b \in B} \mathbf{F}_p^* \cdot b \subset A^*$. This implies the theorem.

For every F of non-zero characteristic p and every $n \in \mathbf{Z}_{\geq 0}$, one readily constructs A and H such that equality holds in the theorem. It is of interest to classify all cases in which the equality sign is valid, and also to drop the commutativity assumption.

An algorithm. The proofs of the unit theorem that we gave in the earlier sections, in the general and in the commutative case, do not offer an efficient method for finding the unit that is asserted to exist. By contrast, the proof that we gave in the present section does lead to an efficient algorithm in the totally split case. It is efficient in the sense that, when sufficiently good algorithms are available for doing arithmetic in the fields involved, it runs in polynomial time.

Resuming the notation used in the first theorem above and its proof, we outline an algorithm that, given a field extension $E \subset F$, a non-negative integer n , and a basis C for F^n over F , constructs a basis B for $W = \sum_{c \in C} E \cdot c$ over E such that $\sum_{b \in B} E^* \cdot b \subset (F^*)^n$.

The algorithm starts by computing E -bases for the subspaces $W_i \subset W$ defined in the proof, as well as bases P_i for the E -vector spaces $\text{Hom}_E(W/W_i, E)$, expressed on a basis for $\text{Hom}_E(W, E)$. For $\rho \in P_i$, write ρ_F for $\rho \otimes \text{id}_F$, which we view as an element of $\text{Hom}_F(W_F, F)$. Let now $\pi_i \in \text{Hom}_F(W_F, F)$ be as in the proof, so that $\pi_1 \wedge \dots \wedge \pi_n \neq 0$. The algorithm finds, for $i = 1, 2, \dots, n$ in succession, an element $\rho_i \in P_i$ such that $\rho_{1F} \wedge \rho_{2F} \wedge \dots \wedge \rho_{iF} \wedge \pi_{i+1} \wedge \dots \wedge \pi_n \neq 0$. This is done as follows. Assume, inductively, that $\rho_{1F} \wedge \rho_{2F} \wedge \dots \wedge \rho_{i-1F} \wedge \pi_i \wedge \pi_{i+1} \wedge \dots \wedge \pi_n \neq 0$. As we saw in the proof, π_i belongs to $\text{Hom}_F(W_F/(W_i)_F, F)$, which is the F -linear span of $(P_i)_F$, so for at least one $\rho \in P_i$ one has $\rho_{1F} \wedge \dots \wedge \rho_{i-1F} \wedge \rho_F \wedge \pi_{i+1} \wedge \dots \wedge \pi_n \neq 0$, or, equivalently, the F -linear map $W_F \longrightarrow F^n$,

$$x \mapsto (\rho_{1F}(x), \dots, \rho_{i-1F}(x), \rho_F(x), \pi_{i+1}(x), \dots, \pi_n(x))$$

is an isomorphism. The first $\rho \in P_i$ that is found to satisfy the latter condition

is chosen to be ρ_i . Once $\rho_1, \rho_2, \dots, \rho_n$ have all been found, one has an isomorphism $W \longrightarrow E^n, x \mapsto (\rho_i(x))_{i=1}^n$ of E -vector spaces. As in the proof, one now takes B to be the inverse image of the standard basis of E^n .

It would be of great interest to extend the algorithm to the non-commutative case.

8. References

Acknowledgements are due to Bas Edixhoven for much of section 7; to Jan Draisma for telling me about Glynn's formula; to Martin Heemskerck for writing [8] and for drawing my attention to the Noether–Deuring theorem; to Lenny Taelman for various useful remarks; and to Abtien Javanpeykar for L^AT_EX help. The Max Planck Institute for Mathematics in Bonn is thanked for its hospitality and its support.

Bibliographic notes. Much of the material in sections 1, 4 and 5 is taken from Martin Heemskerck's bachelor thesis [8]. The combinatorial Nullstellensatz is due to Noga Alon [1]. A particularly short proof was given by Terence Tao [11]. For the theorem of Cauchy–Davenport, see [5, 6, 12]. More about the Jacobson radical can be found in [10, 9]. For descent properties as in section 5, see [3, Ch. VIII, §2.5, Th. 3; 4, Ch. V, Annexe, Prop. 1; 9, Theorem 19.25]. Glynn's determinant formula appeared in [7]. A solution to Exercise 23 can be found in [2].

1. N. Alon, Combinatorial Nullstellensatz, *Combin. Probab. Comput.* **8** (1999), 7–29.
2. E. Artin, *Geometric algebra*, Interscience Publishers, Inc., New York, 1957.
3. N. Bourbaki, *Éléments de mathématique, Algèbre, Chapitre 8*, Springer, Heidelberg, 2012.
4. N. Bourbaki, *Éléments de mathématique, Groupes et algèbres de Lie, Chapitres 4, 5 et 6*, Hermann, Paris, 1968.
5. A. L. Cauchy, *Recherches sur les nombres*, *J. École Polytech.* **9** (1813), 99–116.

6. H. Davenport, *On the addition of residue classes*, J. London Math. Soc. **10** (1935), 30–32.
7. D. G. Glynn, *The modular counterparts of Cayley’s hyperdeterminants*, Bull. Austral. Math. Soc. **57** (1998), 479–492.
8. M. Heemskerk, *Basisuitbreidingen en de Combinatorische Nullstellensatz*, Mathematisch Instituut, Universiteit Leiden, 2014, see:
[HTTPS://WWW.MATH.LEIDENUNIV.NL/SCRIPTIES/HEEMSKERKBACH.PDF](https://www.math.leidenuniv.nl/scripties/heemskerkbach.pdf).
9. T. Y. Lam, *A first course in noncommutative rings*, Springer–Verlag, New York, 1991.
10. S. Lang, *Algebra*, revised third edition, Springer–Verlag, New York, 2002.
11. T. Tao, *Algebraic combinatorial geometry: the polynomial method in arithmetic combinatorics, incidence combinatorics, and number theory*, EMS Surv. Math. Sci. **1** (2014), 1–46.
12. T. Tao, V. Vu, *Additive combinatorics*, Cambridge University Press, Cambridge, 2006.

MATHEMATISCH INSTITUUT, UNIVERSITEIT LEIDEN,
POSTBUS 9512, 2300 RA LEIDEN, NEDERLAND.
hw1@math.leidenuniv.nl