Geometria Algébrica I

lecture 9: Finite-dimensional k-algebras

Misha Verbitsky

IMPA, sala 232

September 17, 2018

Field extensions

DEFINITION: **An extension of a field k** is a field K containing k. We write "K is an extension of k" as $[K:k]$.

DEFINITION: Let $k \subset K$ be a field contained in a field. In this case, we say that k is **a subfield** of K, and K is **extension** of k. An element $x \in K$ is called **algebraic** over K if x is a root of a non-zero polynomial with coefficients in k. An element which is not algebraic is called **transcendental**.

THEOREM: **A sum and a product of algebraic numbers is algebraic.** ■

DEFINITION: A field extension $K \supset k$ is called **algebraic** if all elements of K are algebraic over k. A field k is called **algebraically closed** if all algebraic extensions of k are trivial.

EXAMPLE: **The field $\mathbb{C}$ is algebraically closed.**

DEFINITION: In this lecture, **k-algebra** is a ring containg a field k, not necessarily with unity. **All k-algebras are tacitly assumed commutative.** **Homomorphisms of k-algebras** are k-linear map compatible with the multiplication.

Minimal polynomials

CLAIM: Let K be a finite-dimensional k-algebra with unity and without zero divisors. **Then K is a field.**

Proof: An injective endomorphism of finite-dimensional spaces is surjective. Therefore, for each $x \in K$, there exists $y \in K$ such that $xy = 1$. ■

DEFINITION: Let v be an element of a finite-dimensional k-algebra R, and $P(t) = t^n + a_{n-1}t^{n-1} + \ldots$ a polynomial of smallest possible degree with coefficients in k satisfying $P(v) = 0$. This polynomial is called **the minimal polynomial** of $v \in R$.

CLAIM: Let $v \in R$ be an element of finite-dimensional algebra R over k, and $P(t)$ its minimal polynomial. **Then the subalgebra $R_v \subset R$ generated by v is isomorphic to $k[t]/(P)$.**

Proof: By definition, R_v is a quotient of $k[t]$ by an ideal I of all polynomials $R(t)$ such that $R(v) = 0$. Since $k[t]$ is the principal ideal ring (handout 3), $I = (Q)$ for some polynomial $Q(t)$ satisfying $Q(v) = 0$. **Then Q is the minimal polynomial.** ■

Irreducible polynomials

THEOREM: The polynomial ring $k[t]$ is factorial (admits the unique prime decomposition).

Proof: See handout 3. ■

DEFINITION: A polynomial $P(t) \in k[t]$ is **irreducible** if it is not a product of polynomials $P_1, P_2 \in k[t]$ of positive degree.

PROPOSITION: Let $(P) \subset k[t]$ be a principal ideal generated by the polynomial $P(t)$. Then **the polynomial $P(t)$ is irreducible if and only if the quotient ring $k[t]/(P)$ is a field.**

Proof. Step1: The polynomial P is irreducible if and only if (P) is prime. This follows because $k[t]$ is a factorial ring.

Step 2: The quotient ring $k[t]/(P)$ is finite-dimensional over k. Then, it is a field if and only if it has no zero divisors. ■

Primitive extensions

DEFINITION: Let $P(t) \in k[t]$ be an irreducible polynomial. A field $k[t]/(P)$ is called **an extension of k obtained by adding a root of $P(t)$**. The extension $[k[t]/(P) : k]$ is called **primitive**.

CLAIM: Let $[K : k]$ be a finite extension. **Then K can be obtained from k by a finite chain of primitive extensions**. In other words, there exists a sequence of intermediate extensions $[K = K_n : K_{n-1} : K_{n-2} : ... : K_0 = k]$ such that each $[K_i : K_{i-1}]$ is primitive. ■

Artinian algebras over a field

DEFINITION: A commutative, associative k-algebra R is called **Artinian algebra** if it is finite-dimensional as a vector space over k. Artinian algebra is called **semisimple** if it has no non-zero nilpotents.

DEFINITION: Let $R_1, ..., R_n$ be k-algebras. Consider their direct sum $\oplus R_i$ with the natural (term by term) multiplication and addition. This algebra is called **direct sum of R_i**, and denoted $\oplus R_i$.

Today we are going to prove the following theorem.

THEOREM: Let A be a semisimple Artinian algebra. **Then A is a direct sum of fields, and this decomposition is uniquely defined.**

Idempotents

DEFINITION: Let $v \in R$ be an element of an algebra R satisfying $v^2 = v$. Then v is called **idempotent**.

REMARK: A product of two idemponents is clearly an idempotent. If e is an idemponent, then $1 - e$ is also an idempotent: $(1-e)^2 = 1 - 2e + e^2 = 1 - e$.

COROLLARY: For each idemponent $e \in R$, one has $e(1-e) = 0$. Therefore, **each idemponent $e \in A$ defines a decomposition of A into a direct sum:** $A = eA \oplus (1-e)A$.

All Artinian algebras contain idempotents

THEOREM: Let A be an Artinian k-algebra without nilpotents. **Then A contains an idempotent.**

Proof. Step1: Since A is finite-dimensional, every decreasing chain of ideals stabilizes. Therefore, **A contains an ideal $I \subset A$ which has no non-zero proper ideals**. We shall consider I as a sub-algebra in A.

Step 2: Since A has no nilpotents, for each non-zero $z \in I$ we have $z^2 \neq 0$. Since I is minimal, we have $zI = I$.

Step 3: Since I is finite-dimensional, **all elements of I are invertible as endomorphisms of I.**

Step 4: Since I is finite-dimensional, the elements $z, z^2, z^3, ... \in \operatorname{End} I$ are linearly dependent, which gives a polynomial relation $P(z) = 0$. If this polynomial has zero constant term, we divide it by z, and obtain another polynomial with the same property. Using induction, we obtain a polynomial relation $P(z) = 0$ with non-zero constant term. This gives a relation $\operatorname{Id}_I = az + bz^2 + cz^3 + ...$ in the ring $\operatorname{End}_k(I)$, with $a, b, c, ... \in k$.

Step 5: The element $U := az + bz^2 + cz^3 + ... \in I$ satisfies $Ux = x$ for any $x \in I$. **Therefore, U is an idempotent in A, and unity in I.** ■

Structure theorem for semisimple Artinian algebras

REMARK: Step 5 proves the following useful statement. Let I be a commutative Artinian algebra without zero divisors. **Then I containes unit, that is, I is a field**.

COROLLARY: Let A be a semisimple Artinian algebra, that is, a finite-dimensional commutative k-algebra without nilpotents. **Then A is a direct sum of fields**

Proof: Let $I \subset A$ be a non-trivial ideal. As shown above, I contains a non-zero idempotent a. Then a and $b := 1 - a$ idempotents satisfying $ab = 0$, $a + b = 1$. **This gives a direct sum decomposition $A = aA \oplus (1-a)A$.** Using induction in $\dim A$, we may assume already that aA and $(1-a)A$ are direct sum of fields. ■

Structure theorem for semisimple Artinian algebras: uniqueness of decomposition

LEMMA: Let A be a direct sum of fields, $A = \bigoplus_i k_i$. **Then the decomposition $A = \bigoplus_i k_i$ is defined uniquely**, up to permutation of summands.

Proof: Let $A = \bigoplus_{i=1}^n k_i = \bigoplus_{j=1}^m k'_j$. and $a_1, ..., a_n$, $b_1, ..., b_n$ be the corresponding unipotents. Then the pairwise products $\{a_i b_j\}$ give a family of unipotents which satisfies $\sum a_i b_j = (\sum a_i) \left(\sum b_j\right) = 1$ and $a_i b_j a_{i'} b_{j'} = 0$ unless $i = i', j = j'$. Unless all unipotents $a_i b_j$ are equal to a_i, this gives a direct sum decomposition for each subfield k_i, which is impossible. Therefore, the sets $\{b_j\}$ and $\{a_i\}$ coincide. ■

Finite morphisms

REMARK: Let M be a finitely generated R-module, and $R \longrightarrow R'$ a ring homomorphism. **Then $M \otimes_R R'$ is a finitely generated R'-module**. Indeed, **if M is generated by $x_1, ..., x_n$, then $M \otimes_R R'$ is generated by $x_1, ..., x_n$.**

DEFINITION: A morphism $X \longrightarrow Y$ of affine varieties is called **finite** if the ring $\mathcal{O}_X$ is a finitely generated module over $\mathcal{O}_Y$. In this case, $\mathcal{O}_X$ is called **an integral extension** of $\mathcal{O}_Y$.

THEOREM: Let $X \xrightarrow{f} Y$ be a finite morphism. Then for any point $y \in Y$, **the preimage $f^{-1}(y)$ is finite.**

Proof. Step1: Since $\mathcal{O}_X$ is finite generated as an $\mathcal{O}_Y$-module, the ring $R := \mathcal{O}_X \otimes_{\mathcal{O}_Y} (\mathcal{O}_Y/\mathfrak{m}_y)$ is finitely generated as an $\mathcal{O}_Y/\mathfrak{m}_y$-module. Since $\mathcal{O}_Y/\mathfrak{m}_y = \mathbb{C}$, we obtain that R is an Artinian algebra over $\mathbb{C}$.

Step 2: Let $N \subset R$ be a nilradical. As shown above, Spec(R/N) **is a finite set.**

Step 3: On the other hand, as shown in the last lecture, Spec$(R/N) = f^{-1}(y)$. ■

Bilinear invariant forms

DEFINITION: Let R be a k-algebra, and $g: R \times R \longrightarrow k$ a k-bilinear symmetric form on R. The form g is called **invariant** if $g(x, yz) = g(xy, z)$ for all x, y, $z \in R$.

REMARK: If R has unity, for any invariant form g we have $g(x, y) = h(xy, 1)$, hence g is determined by a linear functional $a \longrightarrow g(a, 1)$.

EXAMPLE: Consider the ring $\mathbb{R}[x,y]/(x^{n+1}, y^{n+1})$, and let $\varepsilon\left(\sum a_{ij}x^i y^j\right) := a_{nn}$. **The corresponding bilinear invariant form $g(x,y) := \varepsilon(xy)$ is non-derenerate (prove this)**.

CLAIM: Let $[K:k]$ be a field extension, and ε a non-zero k-linear functional on K. **Then the bilinear form $g(x,y) := \varepsilon(xy)$ is non-degenerate**.

Proof: Suppose $\varepsilon(a) \neq 0$. Then $g(x, x^{-1}a) \neq 0$. ■

The trace form

DEFINITION: Trace $\operatorname{tr}(A)$ of a linear operator $A \in \operatorname{End}_k(k^n)$ represented by a matrix (a_{ij}) is $\sum_{i=1}^n a_{ii}$.

DEFINITION: Let R be an Artinian algebra over k. Consider the bilinear form $a, b \longrightarrow \operatorname{tr}(ab)$, mapping a, b to the trace of endomorphism $L_{ab} \in \operatorname{End}_k R$, where $l_{ab}(x) = abx$. This form is called **the trace form**, and denoted as $\operatorname{tr}_k(ab)$.

REMARK: Let $[K : k]$ be a finite field extension. As shown above, **the trace form $\operatorname{tr}_k(ab)$ is non-degenerate, unless tr_k is identically 0.**

Separable extensions

DEFINITION: A field extension $[K:k]$ is called **separable** if the trace form $\operatorname{tr}_k(ab)$ is non-zero.

REMARK: **If** $\operatorname{char} k = 0$**, every field extension is separable**, because $\operatorname{tr}_k(1) = \dim_k K$.

THEOREM: Let R be an Artinian algebra over k with non-degenerate trace form. **Then R is semisimple.**

Proof: Since $\operatorname{tr}_k(ab) = 0$ for any nilpotent a (indeed, the trace of a nilpotent operator vanishes), **the ring R contains no non-zero nilpotents**. ■

Tensor product of field extensions

LEMMA: Let R, R' be Artinian k-algebras. Denote the corresponding trace forms by g, g'. Consider the tensor product $R \otimes_k R'$ with a natural structure of Artinian k-algebra. **Then the trace form on $R \otimes_k R'$ is equal $g \otimes g'$,** that is,

$$\operatorname{tr}_{R\otimes_k R'}(x \otimes y, z \otimes t) = g(x, z)g'(y, t). \quad (*)$$

Proof: Let V, W be vector spaces over k, and μ, ρ endomorphisms of V, W. Then $\operatorname{tr}(\mu \otimes \rho) = \operatorname{tr}(\mu)\operatorname{tr}(\rho)$, which is clear from the block decomposition of the matrix $\mu \otimes \rho$. **This gives the trace for any decomposable vector $r \otimes r' \in R \otimes_k R'$.** The equation (*) is extended to the rest of $R \otimes_k R'$ by because decomposable vectors generate $R \otimes_k R'$. ■

COROLLARY: Let $[K_1 : k]$, $[K_2 : k]$ be separable extensions. **Then the Artinian k-algebra $K_1 \otimes_k K_2$ is semisimple,** that is, isomorphic to a direct sum of fields.

Proof: The trace form on $K_1 \otimes_k K_2$ is non-degenerate, because $g \otimes g'$ is non-degenerate whenever g, g' is non-degenerate. ■

REMARK: In particular, **if $\operatorname{char} k = 0$, the product of finite extensions of the field k is always a direct sum of fields.**