Complex analytic spaces

lecture 9: A crash course of Galois theory

Misha Verbitsky

IMPA, sala 236,

September 4, 2023, 13:30

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. We don't assume existence of a unity. 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. Step 1: 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 idempotents. Then the pairwise products $\{a_i b_j\}$ give a family of udempotents 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 udempotents $a_i b_j$ 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. ■

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 $R \otimes_k R'$ 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.**

Tensor product of fields: examples and exercises

PROPOSITION: Let $P(t) \in k[t]$ be a polynomial over k, $[K : k]$ an extension, and $K_1 = k[t]/P(t)$. **Then** $K_1 \otimes K \cong K[t]/P(t)$. ■

COROLLARY: Let $P(t)$ be a polynomial over k, $[K : k]$ an extension, and $K_1 = k[t]/P(t)$. Assume that $P(t)$ is a product of n distinct degree 1 polynomials over K. **Then** $K_1 \otimes K \cong K[t]/P(t) = K^{\oplus n}$.

Proof: Let $P = (t - a_1)(t - a_2)...(t - a_n)$. The natural map $K[t]/(P) \xrightarrow{\tau} \bigoplus_i K[t]/(t - a_i) = K^{\oplus n}K$ is injective, because any polynomial which vanishes in $a_1, a_2, ..., a_n$ is divisible by P. Since the spaces $K[t]/(P)$ and $K[t]/(t - a_i) = K$ are n-dimensional, τ is an isomorphism. ■

REMARK: Surjectivity of τ is known as **"Chinese remainders theorem".**

EXERCISE: Let $P(t) \in \mathbb{Q}[t]$ be a polynomial which has exactly r real roots and $2s$ complex, non-real roots. **Prove that** $(\mathbb{Q}[t]/P) \otimes_{\mathbb{Q}} \mathbb{R} = \bigoplus_s \mathbb{C} \oplus \bigoplus_r \mathbb{R}$.

REMARK: Similarly, **let $P(t) \in k[t]$ be an irreducible polynomial which has irreducible decomposition $P(t) = \prod_i P_i(t)$ in $K[t]$, with all $P_i(t)$ co-prime. Then $k[t]/(P) \otimes_k K \cong K[t]/P(t) \cong \bigoplus_i K[t]/P_i(t)$.** The proof is the same.

Existence of algebraic closure

REMARK: Algebraic closure $[\overline{k} : k]$ is obtained by taking a succession of increasing algebraic extensions, adding to each the roots of irreducible polynomials, and using the Zorn lemma to prove that this will end up in a field which has no non-trivial extensions.

Tensor product of fields and algebraic closure

THEOREM: Let $[\overline{k}:k]$ be the algebraic closure of k, and $[K:k]$ a separable finite extension. **Then $K\otimes_k \overline{k} = \bigoplus \overline{k}$.**

Proof. Step 1: Consider a homomorphism $K \hookrightarrow \overline{k}$, acting as identity on k. Such a homomorphism exists by construction of the algebraic closure. Then

$$K\otimes_k \overline{k} = (K\otimes_k K)\otimes_K \overline{k}$$

by associativity of tensor product.

Step 2: Since $[K:k]$ is separable, $K\otimes_k K = \bigoplus K_i$. **There are at least 2 non-trivial summands in $\bigoplus K_i$,** because for each irreducible polynomial $P(t)\in k[t]$ which has roots in K, one has $K\supset k[t]/(P)$, but $K\otimes_k k[t]/(P) = \bigoplus_i K[t]/(P_i)$, where $P_i(t)\in K[t]$ are irreducible components in the prime decomposition of $P(t)$ over K, with $P(t)=\prod_i P_i(t)$. This gives non-trivial idempotents in $K\otimes_k k[t]/(P)$, hence in $K\otimes_k K\supset K\otimes_k (k[t]/(P))$.

Step 3: By associativity of tensor product,

$$K\otimes_k \overline{k} = (K\otimes_k K)\otimes_K \overline{k} = \bigoplus K_i\otimes_K \overline{k}. \quad (*)$$

Since $\dim_k K = \sum_i \dim_K K_i > \max_i \dim_K K_i$, **the equation $K\otimes_k \overline{k} = \bigoplus \overline{k}$ follows from (*) and induction on $\dim_k K$.** ■

Primitive element theorem

LEMMA: Let k be a field, and $A := \bigoplus_{i=1}^n k$. **Then A contains only finitely many different k-algebras.**

Proof: Let $e_1, ..., e_n$ be the units in the summands of A. Then any idempotent $a \in A$ is a sum of idempotents $a = \sum e_i a$, but $e_i a$ belongs to the i-th summand of A. Then $e_i a = 0$ or $e_i a = e_i$, because k contains only two idempotents. This implies that **any k-algebra $A_i \subset A$ is generated by an idempotent a, which is sum of some a_i.** ■

THEOREM: Let $[K : k]$ be a finite field extension in $\operatorname{char} = 0$. **Then there exists a primitive element $x \in K$,** that is, an element which generates K.

Proof. Step 1: Let $\bar{k}$ be the algebraic closure of k. **The number of intermediate fields $K \supset K' \supset k$ is finite.** Indeed, all such fields correspond to $\bar{k}$-subalgebras in $K \otimes_k \bar{k}$, and **there are finitely many k-subalgebras in $K \otimes_k \bar{k}$ because $K \otimes_k \bar{k} = \bigoplus_i \bar{k}$.**

Step 2: Take for x an element which does not belong to intermediate subfields $K \supsetneq K' \supset k$. Such an element exists, because k is infinite, and K' belong to a finite set of subspaces of positive codimension. **Then x is primitive,** because it generates a subfield which is equal to K. ■