Geometria Algébrica I

lecture 10: Primitive element theorem

Misha Verbitsky

IMPA, sala 232

September 21, 2018

Field extensions (reminder)

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.

Irreducible polynomials (reminder)

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.** ■

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 (reminder)

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 $\oplus R_i$.

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

The trace form (reminder)

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 (reminder)

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 $K_1 \otimes K \cong K[t]/P(t)$.** ■

DEFINITION: Monic polynomial is a polynomial with leading coefficient 1.

COROLLARY: Let $P(t)$ be a monic 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 monic 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, **for any irreducible polynomial $P(t) \in k[t]$ which has an irreducible decomposition $P(t) = \prod_i P_i(t)$ in $K[t]$, with all $P_i(t)$ coprime, one has $k[t]/(P) \otimes_k K \cong K[t]/P(t) \cong \bigoplus_i K[t]/P_i(t)$.** 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. Step1: 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 unipotent $a \in A$ is a sum of unipotents $a = \sum e_i a$, 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 unipotents. This implies that **any k-algebra $A_i \subset A$ is generated by a unipotent 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. Step1: Let $\overline{k}$ be the algebraic closure of k. **The number of intermediate fields $K \supset K' \supset k$ is finite.** Indeed, all such fields correspond to $\overline{k}$-subalgebras in $K \otimes_k \overline{k}$, and **there are finitely many k-subalgebras in $K \otimes_k \overline{k}$ because $K \otimes_k \overline{k} = \bigoplus_i \overline{k}$.**

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. ■

Galois extensions

DEFINITION: Let $[K:k]$ be a finite extension. It is called **a Galois extension** if the algebra $K \otimes_k K$ is isomorphic to a direct sum of several copies of K.

EXERCISE: Let $K = k[t]/(P)$ be a primitive, separable extension, with $\deg P(t) = n$.

1. **Prove that $[K:k]$ is a Galois extension if and only if $P(t)$ has n roots in $K[t]$.**

2. Consider an extension $[K':K]$ obtained by adding all roots of all irreducible components of $P(t) \in K[t]$. **Prove that $[K':k]$ is a Galois extension.**

Galois group

EXERCISE: Let $[K:k]$ be a finite extension, and $G := \operatorname{Aut}_k K$ the group of k-linear automorphisms of K. Prove that $[K:k]$ **is a Galois extension if and only if the set K^G of G-invariant elements of K coincides with k.**

DEFINITION: Let $[K:k]$ be a Galois extension. Then the group $\operatorname{Aut}_k K$ is called **the Galois group of $[K:k]$**.

THEOREM: (Main theorem of Galois theory)
Let $[K:k]$ be a Galois extension, and $\mathcal{G}al_k K$ its Galois group. **Then the subgroups $H \subset \mathcal{G}al_k K$ are in bijective correspondence with the intermediate subfields $k \subset K^H \subset K$,** with K^H obtained as the set of H-invariant elements of K.

EXERCISE: Prove that for any $q = p^n$ there exists a finite field $\mathbb{F}_q$ of q elements. Prove that $[\mathbb{F}_q : \mathbb{F}_p]$ is a Galois extension. Prove that its Galois group is cyclic of order n, and generated by **the Frobenius automorphism** mapping x to x^p.